Mastek
Trust. Value. Velocity

Information Technology (IT) Policy

1. Purpose:

a. The purpose of this policy is to define standards of conduct when employing the use of information technologies for **Mastek Enterprise Solutions Private Ltd.** herein after referred to as the ("MASTEK") by its Board of Directors herein after referred to as the "MANAGEMENT".
b. This IT Policy covers the information technologies including but not limited to, computers, computer files, software, electronic mail, voice mail, entertainment equipment, access control systems, Internet and Intranet.

2. Do's:

a. Use information technologies solely for business purposes of MASTEK
b. Employees should not assume that any computer equipment, technologies of MASTEK, such as electronic mail and data are private and belongs to them. The MASTEK maintains the right and ability to enter these computer systems to access, monitor and review any information. Any Email/data on equipment's provided by the MASTEK is the sole property of MASTEK.
c. MASTEK Signs "Confidentiality & Non-Disclosure Agreements" and/or "Non-Compete Agreements" with its clients. The employees are bound to comply with these agreements back to back.
d. To protect the information contained on the MASTEK enterprise network there have been a number of security measures implemented. Each user is issued a "User Name" and "Password". This password will grant the user access to information based on their job requirements and security level. MASTEK holds the right to restrict access & filter the content.
e. Users must respect the integrity of computing and network systems; for example, users shall not intentionally develop or use programs that harass other users or infiltrate a computer, computing system, or network and/or damage or alter the software components of a computer, computing system or network.
f. Under no circumstances is an employee authorized to engage in any activity that is illegal under local or international law while utilizing the MASTEK owned resources. An employee who suspects or is aware of such activity is required to notify their department head immediately.
g. Surveillance cameras are fitted at various locations for monitoring the movements. All movements are recorded for all 24 hours in a day for security reasons.
h. Network security is a very serious issue. Tampering with data or attempting to circumvent the flow of data is strictly prohibited.
i. Access card and/or biometric finger access as the case may be, is provided to every employee of MASTEK. Employees need to use the access card or biometric finger access strictly for their own entry and exit from various access points. Using the access card or biometric finger access for giving entry or exit for any other person is prohibited and will be treated as breach of IT Policy and liable for punishment as decided by the MANAGEMENT.
j. If an employee creates any liability on behalf of the MASTEK due to inappropriate use of the network, infrastructure and computer systems; the employee agrees to indemnify and hold the MASTEK harmless.
k. Disciplinary action will occur whenever a breach of security or hacking is detected and determined intentional or negligent. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. If you are unsure of any item's appropriateness, consult your department head or operations team.
l. Email signatures must include your name, job title, contact details and the name of MASTEK you work for. You will be provided a standard official signature template to be used in all official Emails sent by you.
m. Strictly adhere to the Email policy and the Email etiquettes. These documents are available for reference on intranet portal, HR and Corporate Affairs Department.
n. MASTEK need to share the data related to any employee or its activities with the Government law enforcement agencies for their investigations upon receipt of a formal request from their competent authority.

o. Freeware under valid General Public License (GPL) may be used with prior management permission.
p. On individual PC, a maximum of One (1) GB storage space is allowed to store the personal data like pay slips and documents which doesn't violate the copyright act restricts individuals storing songs, movies or any other third party software.

3. Don'ts:

The following activities are strictly prohibited:

a. Upload and download of any data which belongs to MASTEK, its partners, clients and business associates. In case of business requirements for such upload and download, employee must take prior written approval of the reporting authority for every instance of said upload and download.
b. Violations of the rights of any person or any MASTEK protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the MASTEK are prohibited.
c. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the MASTEK or the end user does not have an active license is strictly prohibited.
d. Introduction of malicious programs into the network or server (viruses, worms, Trojan horses etc.)
e. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done from home.
f. Using MASTEK computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
g. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. Here, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information.
h. Circumventing user authentication or security of any host, network or account.
i. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet / Intranet / Extranet.
j. Using a removable storage media including the hard disk and other storage media on the system other than those provided by the MASTEK to store files. Bringing external storage devices inside MASTEK premises is prohibited.
k. Sending unsolicited Email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (spam Email).
l. Unauthorized use, or forging, of Email header information.
m. Creating or forwarding "chain letters", or other "pyramid" schemes of any type.
n. Transmission of sensitive information by any employee, by any means of communication including automatic Email forwarding to an address outside the organization is unauthorized unless approved by your department head.
o. Attempting to impersonate any person by using forged headers or other identifying information.
p. Using a proxy server of any kind (other than MASTEK internal proxy server) except unless authorized by management.
q. Attempt to gain access to files and resources to which you have not been granted permission.
r. Steal, vandalize or obstruct the use of computing equipment, facilities, or documentation.
s. You must have no expectation of privacy in anything you create, store, send or receive on the MASTEK computer system. Your Emails can be monitored without prior notification if MASTEK deems this necessary. If there is evidence that you are not adhering to the guidelines set out in this policy, the MASTEK reserves the right to take disciplinary action, including termination and/or appropriate legal action.

t. All Email accounts maintained on our Email systems are property of MASTEK. Passwords should not be given to other people and should be changed once a month. Email accounts not used for 60 days will be deactivated and possibly deleted.
u. Usage of the mobile phones for personal use during the office hours should be need base and brief.
v. Don't listen to songs on network and internet. Don't upload and download songs from internet.

4. MASTEK Acceptable Usage Policy:

Access controls rules and procedures are required to regulate the business functions of MASTEK for ISMS policies are available in MASTEK Intranet portal. These policies apply at all times and should be adhered to whenever accessing MASTEK information technologies and should be used solely for business purpose.

5. Policy Statement:

Each users must read, understand and sign to verify they have read and accepted the policy.

- I understand and agree to comply with the security rules of my organisation.

For the avoidance of doubt, the security rules relating to secure e-mail and information systems usage include:

a. I acknowledge that my usage may be monitored and/or recorded for lawful purposes.
b. I agree to be responsible for any use by me using my unique user credentials (user ID and password, access token or other mechanism as provided) and e-mail address; and,
c. I will not use a colleague's credentials to access MASTEK Information technologies and will equally ensure that my credentials are not shared and are protected against misuse; and,
d. I will protect such credentials at least to the same level of secrecy as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at my employer's premises); and,
e. I will not attempt to access any computer system that I have not been given explicit permission to access; and,
f. I will not transmit information via MASTEK IT that I know or suspect to be unacceptable within the context and purpose for which it is being communicated; and,
g. I will not make false claims or denials relating to my use of MASTEK IT (e.g. falsely denying that an e-mail had been sent or received); and,
h. I will protect any sensitive or not protectively marked material sent, received, stored or processed by me via MASTEK IT to the same level as I would paper copies of similar material; and,
i. I will not send PROTECT or RESTRICTED information over public networks such as Internet; and,
j. I will not forward or disclose any sensitive or PROTECT or RESTRICTED material received via MASTEK IT unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel; and
k. Where IT Services has implemented other measures to protect unauthorized viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked requiring a user logon for reactivation), then I will not attempt to disable such protection; and,
l. I will make myself familiar with MASTEK security policies, procedures and any special instructions that relate to Information Technologies; and,
m. I will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security Information Security Incident Management Policy; and,
n. I will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended; and,
o. I will not remove equipment or information from MASTEK premises without appropriate approval; and,
p. I will take precautions to protect all computer media and portable computers when carrying them outside my organization's premises in accordance with the relevant applicable MASTEK Policy; and,

q. I will not introduce viruses, Trojan horses or other malware into the system; and,
r. I will not disable anti-virus protection provided at my computer; and,
s. I will comply with all other legal, statutory or contractual obligations that MASTEK informs me are relevant; and,
t. If I am about to leave MASTEK, I will inform my manager prior to departure of any important information held in my account and manage my account in accordance with the MASTEK' applicable management policy.

PERSONAL COMMITMENT STATEMENT CUM UNDERTAKING

I, the undersigned, have read policies and understood the business reasons for granting these access rights. I also accept and will abide by this policy, policy statement and all Information Security Policies. I understand that any violation or non - compliance with this Policy may lead to disciplinary, gross misconduct, and/or legal or penal action which may include termination of employment or contractual obligation, civil or criminal prosecution against me by the MANAGEMENT of MASTEK.

EMPLOYEE

Signature: Electronically signed by: Suresh Kumar
Name: Suresh Kumar
Designation: Consultant
Employee Number: CRM
Date: 14/08/2023

AUTHORIZED SIGNATORY (EMPLOYER)

Signature: _____