Information Technology Policy

This Policy applies to all Employee, Contractors, Sub-Contractor of MaRS Planning and Engineering Services Private Limited, its Subsidiaries, Joint Venture Associations and Sister Concerns

Acceptable Use Policy (AUP)

1. Purpose

The purpose of this Acceptable Use Policy (AUP) is to ensure the appropriate use of company information technology resources, including but not limited to computers, networks, internet access, and communication systems, by all employees, contractors, and authorized users of Mars Planning & Engineering Services Pvt. Ltd ("the Company").

2. Scope

This policy applies to all individuals accessing or using the Company's IT resources, regardless of location or device used.

3. Acceptable Use

- All IT resources provided by the Company are to be used for business purposes only.
- Users must comply with all applicable laws and regulations when using Company IT resources.
- Users are responsible for safeguarding their login credentials and must not share them with unauthorized individuals.

- Users must respect the privacy and confidentiality of information stored on Company systems and refrain from unauthorized access or disclosure.
- All software and applications installed on Company devices must be licensed and approved by the IT department.
- Users must refrain from engaging in activities that may disrupt or damage Company systems, including but not limited to spreading malware, hacking, or unauthorized system access.
- Personal use of Company IT resources is permitted within reasonable limits, but should not interfere with work duties or consume excessive bandwidth or storage.

4. Prohibited Activities

The following activities are strictly prohibited:

- Engaging in any form of harassment, discrimination, or illegal activity.
- Accessing, downloading, or distributing illegal or inappropriate content, including but not limited to pornography, hate speech, or copyrighted material without proper authorization.
- Sending unsolicited commercial emails (spam), chain letters, or any other form of unauthorized communication.
- Using Company IT resources for personal financial gain or for promoting personal business interests without prior approval.
- Circumventing or attempting to circumvent security controls or engaging in unauthorized attempts to access restricted areas or data.
- Installing unauthorized software, including but not limited to games, file-sharing programs, or malicious software.
- Sharing confidential or proprietary Company information with unauthorized individuals or third parties.

5. Monitoring and Enforcement

The Company reserves the right to monitor, access, and review all activities conducted on its IT resources to ensure compliance with this policy. Violations of this policy may result in disciplinary action, up to and including termination of employment or legal action.

6. Reporting Violations

Users who become aware of any violations of this policy or suspicious activities on Company IT resources must report them immediately to the IT department or designated authorities.

7. Policy Review

This policy will be reviewed periodically and updated as necessary to reflect changes in technology, business practices, or regulatory requirements.

8. Acknowledgment

By accessing or using Company IT resources, users acknowledge that they have read, understood, and agree to comply with this Acceptable Use Policy.

Information Security Policy

1. Purpose

The purpose of this Information Security Policy (ISP) is to establish guidelines and procedures for protecting the confidentiality, integrity, and availability of company information assets, including but not limited to data, systems, and networks, within Mars Planning & Engineering Services Pvt. Ltd ("the Company").

2. Scope

This policy applies to all employees, contractors, vendors, and third parties who have access to or handle company information assets, regardless of location or device used.

3. Information Classification

- Company information assets shall be classified based on their sensitivity level, including but not limited to confidential, internal use only, and public information.
- Employees shall adhere to data classification guidelines and handle information according to its designated classification level.

4. Access Control

- Access to company information assets shall be granted based on the principle of least privilege, ensuring that users have only the minimum level of access necessary to perform their job duties.
- User access rights shall be reviewed regularly and revoked or modified as needed, especially upon changes in job roles or termination of employment.
- No Employee is allowed to use any external device or transfer confidential document from Company computer to personal devices or online portal without consent of IT team.

5. Data Protection

- Company data shall be protected through appropriate technical and organizational measures, including encryption, access controls, and data loss prevention mechanisms.
- Employees shall handle and transmit sensitive information securely, following encryption standards and secure communication protocols.

6. Security Awareness and Training

- All employees shall receive regular training and awareness programs on information security best practices, including phishing awareness, password management, and data handling procedures.
- Employees shall be required to acknowledge their understanding of security policies and their commitment to comply with them.

7. Incident Response

- Procedures shall be established for detecting, reporting, and responding to security incidents, including data breaches, malware infections, and unauthorized access attempts.
- An incident response team shall be designated and trained to handle security incidents promptly and effectively, following predefined incident response procedures.

8. Physical Security

- Physical access to company facilities, server rooms, and data centers shall be restricted to authorized personnel only, using access controls, surveillance, and environmental controls.
- Measures shall be implemented to protect IT equipment and assets from theft, vandalism, or unauthorized access.

9. Vendor Management

- Third-party vendors and service providers shall be selected based on their ability to meet security requirements and shall be subject to contractual agreements ensuring compliance with security standards.
- Regular assessments and audits shall be conducted to evaluate the security posture of vendors and mitigate any potential security risks.

10. Compliance and Legal Requirements

- The Company shall comply with all applicable laws, regulations, and industry standards related to information security, privacy, and data protection.
- Regular audits and assessments shall be conducted to ensure compliance with security requirements and address any identified vulnerabilities or non-compliance issues.

11. Policy Review

- This policy shall be reviewed periodically and updated as necessary to reflect changes in technology, business practices, or regulatory requirements.
- Employees shall be notified of any changes to the Information Security Policy and provided with training or guidance as needed to ensure compliance.

12. Acknowledgment

- All employees, contractors, and third parties with access to company information assets shall acknowledge their understanding of this Information Security Policy and their commitment to comply with its requirements.

Password Policy

1. Purpose

The purpose of this Password Policy is to establish guidelines and best practices for creating, managing, and protecting passwords to ensure the security of company information assets within Mars Planning & Engineering Services Pvt. Ltd ("the Company").

2. Scope

This policy applies to all employees, contractors, vendors, and third parties who have access to company IT resources, including but not limited to computers, networks, and applications.

3. Password Creation

- Passwords must be at least [8] characters long. (Recommendation: 12 characters or more)
- Passwords must contain a combination of uppercase and lowercase letters, numbers, and special characters.
- Passwords must not be based on easily guessable information, such as dictionary words, names, or common phrases.
- Users should avoid using the same password for multiple accounts or systems.

4. Password Management

- Users must not share their passwords with anyone, including coworkers or IT staff.
- Passwords must be changed at least every [60] days. (Recommendation: 90 days)
- Passwords must be changed immediately if there is suspicion of compromise or unauthorized access.
- Users must not write down passwords or store them in unsecured locations, such as sticky notes or unprotected digital files.

5. Password Storage and Transmission

- Passwords must be stored securely using industry-standard encryption algorithms and practices.

- Passwords must not be transmitted over insecure channels, such as email or instant messaging, unless encrypted.

6. Multi-Factor Authentication (MFA)

- Multi-factor authentication (MFA) must be enabled for all systems and applications where technically feasible.
- MFA should use at least two independent factors, such as passwords, biometrics, or security tokens.

7. Account Lockout

- Accounts must be locked out after a specified number of unsuccessful login attempts to prevent brute-force attacks.
- Locked accounts must be unlocked by authorized personnel after proper identity verification.

8. Password Recovery

- Procedures must be established for securely recovering or resetting passwords in case of forgotten passwords or account lockout.
- Password recovery mechanisms must require proper identity verification and follow established security protocols.

9. Monitoring and Enforcement

- The IT department shall monitor password usage and compliance with this policy to identify any security vulnerabilities or non-compliance issues.
- Violations of this policy may result in disciplinary action, up to and including termination of employment.

10. Policy Review

- This policy shall be reviewed periodically and updated as necessary to reflect changes in technology, security threats, or business requirements.
- Employees shall be notified of any changes to the Password Policy and provided with training or guidance as needed to ensure compliance.

11. Acknowledgment

- All employees, contractors, and third parties with access to company IT resources shall acknowledge their understanding of this Password Policy and their commitment to comply with its requirements.

Data Backup and Recovery Policy

1. Purpose

The purpose of this Data Backup and Recovery Policy is to establish guidelines and procedures for the backup, storage, and recovery of company data to ensure its availability, integrity, and confidentiality within Mars Planning & Engineering Services Pvt. Ltd ("the Company").

2. Scope

This policy applies to all employees, contractors, vendors, and third parties who have access to or handle company data, regardless of location or device used.

3. Data Backup Procedures

- Regular backups of company data shall be performed according to predefined schedules and backup policies.
- Backups shall include all critical data, including but not limited to databases, applications, user files, and configuration settings.
- Backup frequency and retention periods shall be defined based on data criticality, regulatory requirements, and business needs.

4. Backup Storage

- Backup data shall be stored securely in offsite or cloud-based locations to protect against data loss due to local hardware failures, disasters, or cyberattacks.
- Backup storage locations shall be geographically diverse to mitigate risks associated with regional disasters or disruptions.

5. Data Recovery Procedures

- Procedures shall be established for timely and efficient data recovery in the event of data loss or corruption.
- Recovery point objectives (RPOs) and recovery time objectives (RTOs) shall be defined for each critical system or data set to ensure timely restoration of service.

6. Backup Testing and Validation

- Regular testing and validation of backup systems and procedures shall be conducted to ensure data integrity and recoverability.
- Backup and recovery tests shall include simulated disaster scenarios to assess the effectiveness of recovery procedures.

7. Disaster Recovery Plan (DRP)

- A comprehensive disaster recovery plan shall be developed and maintained to guide the response and recovery efforts in the event of a catastrophic failure or disaster.
- The disaster recovery plan shall include predefined roles and responsibilities, communication protocols, and escalation procedures.

8. Security and Encryption

- Backup data shall be encrypted during transmission and storage to protect against unauthorized access or disclosure.
- Encryption keys shall be managed securely and independently from the backup data to prevent unauthorized decryption.

9. Monitoring and Auditing

- Backup systems and procedures shall be monitored regularly to ensure compliance with this policy and identify any potential issues or vulnerabilities.
- Regular audits and reviews of backup logs and reports shall be conducted to verify adherence to backup schedules and validate data integrity.

10. Policy Review

- This policy shall be reviewed periodically and updated as necessary to reflect changes in technology, business requirements, or regulatory requirements.
- Employees shall be notified of any changes to the Data Backup and Recovery Policy and provided with training or guidance as needed to ensure compliance.

11. Acknowledgment

- All employees, contractors, and third parties with access to company data shall acknowledge their understanding of this Data Backup and Recovery Policy and their commitment to comply with its requirements.

Network Security Policy

1. Purpose

The purpose of this Network Security Policy is to establish guidelines and procedures for securing the company's network infrastructure to protect against unauthorized access, data breaches, and cyber threats within Mars Planning & Engineering Services Pvt. Ltd ("the Company").

2. Scope

This policy applies to all employees, contractors, vendors, and third parties who have access to or use the company's network resources, including but not limited to wired and wireless networks, routers, switches, and firewalls.

3. Network Access Control

- Access to the company's network resources shall be restricted to authorized users and devices only.
- Users and devices shall be authenticated using strong authentication mechanisms, such as usernames, passwords, and multi-factor authentication (MFA).

4. Firewall Configuration

- Firewalls shall be deployed and configured to monitor and control incoming and outgoing network traffic based on predefined security policies.
- Firewall rules shall be regularly reviewed and updated to reflect changes in business requirements and security threats.

5. Intrusion Detection and Prevention

- Intrusion detection and prevention systems (IDPS) shall be implemented to detect and block suspicious network activities and unauthorized access attempts.
- IDPS logs and alerts shall be monitored regularly to identify and respond to potential security incidents.

6. Wireless Network Security

- Wireless networks shall be secured using encryption protocols, such as WPA2 or WPA3, to protect against eavesdropping and unauthorized access.
- Wireless access points shall be configured with strong passwords and access controls to prevent unauthorized connections.

7. Network Segmentation

- Network segmentation shall be implemented to isolate sensitive systems and data from untrusted network segments and mitigate the impact of security breaches.
- Access controls and firewall rules shall be enforced to restrict communication between network segments based on least privilege principles.

8. Remote Access Security

- Remote access to the company's network resources shall be protected using secure VPN connections and strong authentication methods, such as certificates or token-based authentication.
- Remote access sessions shall be encrypted to ensure confidentiality and integrity of data transmitted over the network.

9. Monitoring and Logging

- Network traffic shall be monitored continuously to detect and analyze security events, anomalies, and unauthorized activities.
- Network logs shall be retained for a predefined period to support incident response, forensic analysis, and compliance requirements.

10. Policy Review

- This policy shall be reviewed periodically and updated as necessary to reflect changes in technology, business requirements, or regulatory requirements.
- Employees shall be notified of any changes to the Network Security Policy and provided with training or guidance as needed to ensure compliance.

11. Acknowledgment

- All employees, contractors, and third parties with access to the company's network resources shall acknowledge their understanding of this Network Security Policy and their commitment to comply with its requirements.

Software Licensing Policy

1. Purpose

The purpose of this Software Licensing Policy is to establish guidelines and procedures for the acquisition, deployment, and management of software licenses within Mars Planning & Engineering Services Pvt. Ltd ("the Company").

2. Scope

This policy applies to all employees, contractors, vendors, and third parties who have access to or use company-owned software applications and systems.

3. Software Acquisition

- Software licenses shall be acquired through authorized channels and vendors in compliance with applicable licensing agreements and regulations.
- The IT department shall maintain an inventory of all software licenses, including license keys, purchase records, and renewal dates.

4. License Compliance

- Employees shall use software applications in accordance with the terms and conditions of their respective licensing agreements.
- Unauthorized copying, distribution, or use of software without a valid license is strictly prohibited.

5. License Activation and Installation

- Software licenses shall be activated and installed only on authorized devices and for authorized users.
- Installation of software on personal devices for work purposes (BYOD) shall comply with the company's BYOD policy and software licensing agreements.

6. License Renewal and Maintenance

- Software licenses shall be renewed or extended in a timely manner to ensure uninterrupted access to software updates, patches, and technical support.

- The IT department shall monitor license expiration dates and coordinate license renewal or procurement as needed.

7. License Audits and Compliance Checks

- Regular audits and compliance checks shall be conducted to verify software license usage and ensure compliance with licensing agreements.
- Non-compliance with software licensing agreements may result in disciplinary action or legal consequences for individuals or the company.

8. Software Usage Monitoring

- Usage of licensed software applications shall be monitored to identify underutilized licenses, optimize license allocation, and avoid unnecessary expenses.
- License usage reports and metrics shall be reviewed periodically to support decision-making and license optimization efforts.

9. Policy Review

- This policy shall be reviewed periodically and updated as necessary to reflect changes in technology, software usage patterns, or licensing requirements.
- Employees shall be notified of any changes to the Software Licensing Policy and provided with training or guidance as needed to ensure compliance.

10. Acknowledgment

- All employees, contractors, and third parties with access to company-owned software applications shall acknowledge their understanding of this Software Licensing Policy and their commitment to comply with its requirements.

Remote Access Policy

1. Purpose

The purpose of this Remote Access Policy is to establish guidelines and procedures for secure remote access to company resources to ensure the confidentiality, integrity, and availability of data within Mars Planning & Engineering Services Pvt. Ltd ("the Company").

2. Scope

This policy applies to all employees, contractors, vendors, and third parties who require remote access to company systems, networks, or data.

3. Remote Access Methods

- Remote access to company resources shall be provided through secure virtual private network (VPN) connections, remote desktop services, or other approved remote access technologies.
- Only authorized devices and users with valid credentials shall be granted remote access privileges.

4. Authentication and Authorization

- Remote access users shall be authenticated using strong authentication methods, such as passwords, biometrics, or multi-factor authentication (MFA).
- Access permissions shall be granted based on the principle of least privilege, ensuring that users have only the minimum level of access necessary to perform their job duties.

5. Encryption and Security Controls

- Remote access sessions shall be encrypted using industry-standard encryption protocols, such as SSL/TLS, to protect data in transit from unauthorized interception or eavesdropping.
- Security controls, such as firewalls, intrusion detection systems, and endpoint security solutions, shall be implemented to detect and prevent unauthorized access or malicious activities.

6. Device Security

- Devices used for remote access, including laptops, smartphones, and tablets, shall be configured with up-to-date security patches, antivirus software, and encryption mechanisms to protect against malware and data breaches.
- Lost or stolen devices used for remote access must be reported immediately to the IT department to initiate appropriate security measures, such as remote wipe or device lockdown.

7. Monitoring and Logging

- Remote access sessions shall be monitored and logged to track user activity, detect security incidents, and support forensic investigations.
- Logs of remote access activities shall be retained for a predefined period in accordance with data retention policies and regulatory requirements.

8. Compliance and Policy Enforcement

- Remote access users shall comply with all applicable company policies, including but not limited to acceptable use policies, security policies, and data protection policies.
- Violations of this policy may result in disciplinary action, up to and including termination of employment or legal action.

9. Policy Review

- This policy shall be reviewed periodically and updated as necessary to reflect changes in technology, business requirements, or regulatory requirements.
- Employees shall be notified of any changes to the Remote Access Policy and provided with training or guidance as needed to ensure compliance.

10. Acknowledgment

- All employees, contractors, and third parties with remote access privileges shall acknowledge their understanding of this Remote Access Policy and their commitment to comply with its requirements.

Email and Communication Policy

1. Purpose

The purpose of this Email and Communication Policy is to establish guidelines and best practices for the appropriate use of company email and communication systems to ensure effective communication, data security, and compliance within Mars Planning & Engineering Services Pvt. Ltd ("the Company").

2. Scope

This policy applies to all employees, contractors, vendors, and third parties who use company email and communication systems for business purposes.

3. Acceptable Use

- Company email and communication systems shall be used for official business purposes only and shall not be used for personal or non-business-related activities.
- Users shall exercise professional judgment and discretion when communicating via company email and communication channels, adhering to company values and standards of conduct.

4. Data Protection and Confidentiality

- Users shall not disclose sensitive or confidential information via company email or communication channels unless authorized to do so.
- Emails containing sensitive information shall be encrypted when transmitted over public networks or to external recipients.

5. Email Security

- Users shall be cautious of phishing emails, suspicious attachments, and links, and shall report any suspicious emails to the IT department or designated authorities.
- Email attachments shall be scanned for malware and viruses before opening or downloading them to prevent security breaches.

6. Email Retention and Archiving

- Company email messages shall be retained and archived in accordance with company policies, industry regulations, and legal requirements.
- Users shall comply with email retention policies and refrain from deleting or altering emails that are subject to retention requirements.

7. Email Monitoring and Compliance

- Company email and communication systems may be monitored for compliance with this policy, security purposes, and legal or regulatory requirements.
- Users shall have no expectation of privacy when using company email and communication channels and shall consent to monitoring and compliance checks.

8. Personal Email Use

- Limited personal use of company email may be permitted within reasonable limits, but shall not interfere with work duties or violate company policies.
- Personal emails sent or received via company email systems shall not contain offensive, inappropriate, or illegal content.

9. Policy Review

- This policy shall be reviewed periodically and updated as necessary to reflect changes in technology, business requirements, or regulatory requirements.
- Employees shall be notified of any changes to the Email and Communication Policy and provided with training or guidance as needed to ensure compliance.

10. Acknowledgment

- All employees, contractors, and third parties who use company email and communication systems shall acknowledge their understanding of this Email and Communication Policy and their commitment to comply with its requirements.

Vendor Management Policy

1. Purpose

The purpose of this Vendor Management Policy is to establish guidelines and procedures for managing relationships with third-party vendors and service providers to ensure compliance, security, and quality within Mars Planning & Engineering Services Pvt. Ltd ("the Company").

2. Scope

This policy applies to all employees, contractors, and departments involved in the selection, engagement, and oversight of third-party vendors and service providers on behalf of the company.

3. Vendor Selection and Evaluation

- Vendors shall be selected based on predefined criteria, including but not limited to qualifications, experience, reputation, financial stability, and compliance with regulatory requirements.
- Vendor evaluations shall be conducted periodically to assess performance, service quality, and adherence to contractual obligations.

4. Contract Management

- Written contracts or agreements shall be established with all vendors, outlining the terms and conditions of the engagement, including scope of work, deliverables, pricing, service levels, and termination clauses.
- Contracts shall include provisions addressing data protection, confidentiality, security, and compliance with applicable laws and regulations.

5. Security and Compliance

- Vendors shall be required to comply with company security policies, data protection requirements, and industry standards for information security.
- Vendors shall be subject to security assessments, audits, and compliance checks to verify adherence to security standards and contractual obligations.

6. Risk Management

- Risks associated with vendor relationships, including but not limited to financial, operational, legal, and reputational risks, shall be assessed and mitigated through appropriate risk management strategies.
- Risk assessments shall be conducted during vendor selection, contract negotiation, and throughout the duration of the vendor relationship.

7. Performance Monitoring

- Vendor performance shall be monitored regularly to ensure compliance with contractual agreements, service level agreements (SLAs), and performance metrics.
- Key performance indicators (KPIs) shall be established to measure vendor performance and identify areas for improvement or corrective action.

8. Vendor Oversight and Governance

- A designated vendor management team or individual shall be responsible for overseeing vendor relationships, resolving issues, and maintaining communication with vendors.
- Regular meetings and reviews shall be conducted with vendors to discuss performance, address