



MONOMARK ENGINEERING (INDIA) LIMITED

INFORMATION TECHNOLOGY AND CYBERSECURITY POLICY

1. PURPOSE

The purpose of this Information Technology and Cybersecurity Policy ("Policy") is to establish a framework for the secure, reliable and efficient use and management of the information technology resources of **Monomark Engineering India Limited** ("Company").

The Policy is intended to protect the Company's information and technology assets, maintain the confidentiality, integrity and availability of business information, support business continuity and establish appropriate responsibilities and controls for the use of information technology resources.

The Company is committed to adopting reasonable and appropriate measures to safeguard its information systems and technology infrastructure against unauthorized access, misuse, loss, disruption and other cybersecurity risks.

2. SCOPE

This Policy shall apply to all employees, officers, consultants, contractors, temporary staff, vendors, service providers and other authorized users who access or use the Company's information technology resources.

The Policy shall cover, as applicable:

- Company-owned or Company-controlled computers, laptops, servers, network equipment, printers and storage devices;
- Enterprise resource planning (ERP) systems and other business applications;
- Official email and other communication platforms;
- Internet, Wi-Fi, VPN, firewall and remote-access facilities;
- Cloud-based applications and digital platforms approved by the Company;
- Company information, electronic records, databases and digital documents;
- Backup systems, logs, credentials and other technology-related information; and
- IT and network infrastructure supporting security and surveillance systems installed at Company premises.

3. GOVERNANCE AND RESPONSIBILITIES

3.1 Management



The management shall provide appropriate oversight for the Company's IT and cybersecurity framework and ensure that reasonable resources and controls are available for protecting the Company's information and technology infrastructure.

3.2 IT Function

The IT function, whether managed internally or through an authorized service provider, shall be responsible for:

- Maintaining the Company's IT infrastructure and systems;
- Implementing appropriate information security controls;
- Managing user accounts, access rights and IT assets;
- Maintaining system updates, backups and security measures;
- Monitoring and addressing IT and cybersecurity incidents;
- Maintaining appropriate records relating to IT assets, access and incidents; and
- Periodically reviewing IT systems and security controls and recommending improvements.

3.3 Department Heads / Process Owners

Department Heads and Process Owners shall:

- Ensure that access provided to employees is appropriate for their roles and responsibilities;
- Approve business requirements for access to systems and information;
- Ensure compliance with this Policy within their respective functions; and
- Promptly communicate employee transfers, changes in responsibilities and separations to the relevant functions.

3.4 Employees and Authorized Users

All users of Company IT resources shall:

- Use Company IT resources responsibly and for authorized purposes;
- Protect Company information, passwords and assigned devices;
- Follow applicable information security requirements;
- Report suspected cybersecurity incidents, loss or theft of devices, phishing attempts or unauthorized access promptly; and
- Refrain from bypassing or disabling security controls implemented by the Company.

4. IT ASSET MANAGEMENT

The Company shall maintain appropriate records of its IT assets, including computers, laptops, servers, network equipment and other technology assets, as considered appropriate.

IT assets shall be allocated to authorized users against appropriate acknowledgement or handover records.

Users shall exercise reasonable care in handling Company-owned IT assets. Any loss, theft, damage or unauthorized use of Company IT assets shall be reported promptly to the concerned authority and IT function.

Transfer, replacement, repair, disposal or write-off of IT assets shall be carried out in accordance with the Company's applicable procedures and approval requirements.



5. ACCESS CONTROL AND USER ACCOUNTS

Access to Company systems, applications and information shall be provided based on business requirements, job responsibilities and appropriate authorization.

The Company shall follow the principle of least privilege, whereby users shall be provided only such access as is reasonably required for performing their duties.

Administrative and privileged access shall be restricted to authorized personnel.

User access shall be reviewed periodically and whenever there is a change in role, responsibility or employment status.

Access to Company systems shall be disabled or appropriately modified upon separation from the Company or when such access is no longer required.

6. PASSWORD AND AUTHENTICATION

Users shall maintain the confidentiality of their passwords and authentication credentials and shall not share them with any other person.

Passwords should be appropriately strong, unique and changed whenever there is a reasonable suspicion of compromise.

Multi-factor authentication ("MFA") may be implemented for critical systems, privileged accounts and other systems wherever reasonably feasible.

Any suspected compromise of passwords or authentication credentials shall be reported to the IT function without undue delay.

7. E-MAIL, INTERNET AND COMMUNICATION RESOURCES

Company-provided email and communication facilities shall primarily be used for legitimate business purposes.

Users shall exercise caution while opening links, attachments or messages received from unknown or suspicious sources.

Users shall not knowingly use Company systems for unlawful, fraudulent, offensive or unauthorized activities.

Confidential or sensitive Company information shall not be forwarded to personal email accounts or shared through unauthorized communication platforms.



The Company may monitor or restrict the use of its IT and network resources to the extent permitted under applicable laws and Company requirements, particularly for security, compliance and operational purposes.

8. INFORMATION AND DATA SECURITY

Company information shall be classified and handled with an appropriate level of care based on its sensitivity and business importance.

Confidential and sensitive information shall be stored, transmitted and shared only through Company-approved systems and channels.

Users shall take reasonable precautions to prevent unauthorized access, disclosure, alteration, loss or destruction of Company information.

Company information shall not be copied to personal devices, unauthorized cloud storage or other unapproved locations without appropriate authorization.

9. ENDPOINT AND DEVICE SECURITY

Company computers, laptops and other devices shall use appropriate security controls, including supported operating systems, security updates and endpoint protection, as applicable.

Users shall lock or secure their devices when left unattended.

Installation of unauthorized, pirated, counterfeit or unlicensed software on Company devices is prohibited.

Users shall not disable or circumvent security software, system controls or other security measures implemented by the Company.

Use of removable storage devices shall be subject to business requirements and applicable security controls.

10. NETWORK AND REMOTE ACCESS

Network infrastructure, firewalls and other security configurations shall be managed only by authorized personnel or approved service providers.

Remote access to Company systems shall be provided only where there is a legitimate business requirement and appropriate security controls are in place.

VPN or other approved secure connectivity mechanisms shall be used where required for remote access to Company systems.

Users shall not share network credentials or provide unauthorized persons access to Company networks.



11. BACKUP AND BUSINESS CONTINUITY

The Company shall maintain appropriate backup arrangements for critical business information and systems, based on business requirements.

Access to backups shall be restricted to authorized personnel.

The IT function shall monitor backup processes and, where appropriate, periodically verify the availability and recoverability of critical backups.

The Company shall endeavour to maintain appropriate IT arrangements to support business continuity and recovery in the event of system failure, cyber incidents, data loss or other disruptions.

12. BUSINESS APPLICATIONS AND ERP SYSTEMS

Access to ERP and other business applications shall be provided based on approved roles and responsibilities.

Users shall not use another person's credentials or permit another person to use their assigned credentials.

Access rights shall be reviewed periodically and upon changes in roles or responsibilities.

Where reasonably practicable, the Company shall seek to identify and address excessive, conflicting or inappropriate access rights.

13. SOFTWARE LICENSING AND IT PROCUREMENT

The Company shall use genuine, licensed and appropriately authorized software and technology solutions.

Procurement of IT hardware, software, subscriptions and services shall be undertaken in accordance with the Company's applicable procurement and approval processes.

Appropriate records of software licenses, subscriptions, warranties and support arrangements shall be maintained, where applicable.

14. CYBERSECURITY AND INCIDENT MANAGEMENT

The Company shall maintain reasonable measures to identify, prevent, detect and respond to cybersecurity threats and incidents.

Cybersecurity incidents may include, among other things:

- Phishing and social engineering attacks;
- Malware or ransomware incidents;
- Unauthorized access;



- Data loss or unauthorized disclosure;
- Compromise of user credentials;
- Loss or theft of IT devices; and
- Significant disruption to IT systems or services.

Any suspected or actual cybersecurity incident shall be reported promptly to the IT function and/or the appropriate reporting authority.

Material incidents shall be appropriately investigated, documented and escalated to management, where necessary.

15. EMPLOYEE JOINING, TRANSFER AND EXIT

The Company shall maintain appropriate IT access and asset management processes in connection with employee joining, transfer and separation.

Upon joining, relevant users may be provided with authorized system access and Company IT assets based on their role and business requirements.

Upon transfer, access rights, system roles and asset allocation shall be reviewed and updated as appropriate.

Upon separation, Company IT assets shall be recovered and system access shall be disabled or revoked in coordination with the relevant functions.

16. REMOTE WORKING AND USE OF PERSONAL DEVICES

Where employees are permitted to work remotely, they shall ensure that Company information and IT assets are used in a secure manner.

Company devices shall be protected against unauthorized access, loss or theft while being used outside Company premises.

Use of personal devices for accessing Company systems or information shall be permitted only where authorized by the Company and subject to applicable security requirements.

Company information shall not be stored on personal devices or personal cloud storage without appropriate authorization.

17. THIRD-PARTY ACCESS

Third-party service providers, consultants and vendors requiring access to Company systems or information shall be provided access only to the extent necessary for the approved purpose.

Where appropriate, third-party access shall be subject to contractual confidentiality, information security and data protection requirements.



Third-party access shall be reviewed and withdrawn when the relevant engagement or business requirement ends.

18. IT AWARENESS AND EMPLOYEE RESPONSIBILITY

The Company shall endeavour to promote awareness among employees regarding information security and cybersecurity risks.

Employees are expected to remain vigilant against phishing, fraudulent payment requests, suspicious communications, malware and other cybersecurity threats.

Employees shall cooperate with reasonable IT security assessments, investigations, awareness initiatives and corrective measures undertaken by the Company.

19. MONITORING AND REVIEW

The Company may conduct periodic reviews of its IT infrastructure, user access, IT assets, cybersecurity controls and compliance with this Policy.

Appropriate logs, records and system information may be maintained and reviewed for legitimate business, security, audit and compliance purposes, subject to applicable laws and Company requirements.

20. POLICY VIOLATIONS

Any violation of this Policy may be reviewed by the Company and appropriate corrective or disciplinary action may be taken in accordance with applicable laws and Company policies.

Serious or material violations, including unauthorized access, deliberate misuse of Company information or technology resources, data theft or intentional circumvention of security controls, may be escalated to the appropriate level of management.

21. COMPLIANCE WITH APPLICABLE LAWS

The Company shall endeavour to comply with applicable laws, regulations and regulatory requirements relating to information technology, cybersecurity, data protection and electronic records, as applicable to its business and operations.

Nothing contained in this Policy shall restrict the Company from implementing additional controls or procedures where required to meet applicable legal, regulatory, contractual or business requirements.

22. REVIEW OF POLICY

This Policy shall be reviewed periodically and may be amended from time to time to reflect changes in the Company's business operations, technology environment, cybersecurity risks, applicable laws and regulatory requirements.

