Approval

The signatures below certify that this management system policy has been reviewed and accepted, and demonstrates that the signatories are aware of all the requirements contained herein and are committed to ensuring their provision.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Name | Signature | Position | Date |
| Prepared by | Dhairyasheel Ashok Mulik Patil |  | Quality Manager |  |
| Reviewed by | Dr Prveen Bidare |  | Senior Engineer |  |
| Approved by | Joyti Bidare |  | CEO |  |

Amendment Record

This procedure is reviewed to ensure its continuing relevance to the systems and process that it describes. A record of contextual additions or omissions is given below:

|  |  |  |  |
| --- | --- | --- | --- |
| Page No. | Context | Revision | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Company Proprietary Information

The electronic version of this procedure is the latest revision. It is the responsibility of the individual to ensure that any paper material is the current revision. The printed version of this manual is uncontrolled, except when provided with a document reference number and revision in the field below:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Document Ref. |  | | | | | Rev |  |
|  |  |  | | | |  |  |
| Uncontrolled Copy |  |  | Controlled Copy |  |  | Date |  |

**Technology Policy**

***1. Purpose***

The purpose of this Technology Policy is to establish clear guidelines for the responsible use, management, and security of technology at Manufacturing Made Easy Ltd (MME Ltd). This policy ensures data protection, operational continuity, and compliance with industry standards while optimizing the use of CAD/CAM software for product design and development.

***2. Scope***

This policy applies to all employees, suppliers, and third parties who might have access to MME Ltd.’s technology infrastructure, including but not limited to:

* Computer hardware and software
* Network and internet usage
* Data storage and protection
* AI usage limitations
* Cybersecurity measures

***3. Software Usage and Updates***

* MME Ltd primarily uses CAD/CAM software for product design and development.
* All software must be licensed and approved by Top management.
* Six months software review will be conducted to determine necessary updates, ensuring technological advancement.
* Unapproved software installations are strictly prohibited to mitigate security risks. A security PIN must be entered before installing any software, and this PIN will be accessible only to Top management.
* All employees will receive Microsoft 360 Business to support their work and enhance productivity.
* Company email must be used exclusively for official business communications and work-related tasks.

***4. AI Protocol***

* The use of Gen AI in financial matters is strictly prohibited to prevent inaccuracies, security risks, and potential leaks of important financial data outside the organization.
* Gen AI tools must not be used for sharing, processing, or modifying product design documents, including CAD/CAM files and other critical design-related documents, unless explicitly authorized by senior management.
* Employees must consult with the Quality Manager or Senior Engineer before integrating Gen AI solutions into workflows.

***5. Data Protection and Backup***

* Critical documents (design files, client data, contracts, etc.) must be stored securely with restricted access.
* Data backup procedures include:
  + Daily cloud backups to OneDrive.
  + Weekly physical backups of relevant QMS documents on an encrypted hard drive or pen drive, stored securely in a company safe.
* Folder lock encryption must be applied to critical files.
* Individual computer lock policies must be enforced on all employee laptops and PCs.

***6. Data Loss Prevention (DLP) Protocol***

* Employees must immediately report any data loss or suspected security breach to the Quality Manager.
* Data loss incidents will be assessed, and necessary steps will be taken to recover data, including outsourcing for tech-related issues or events when needed.
* Unauthorized access, downloading, or transmission of sensitive files is strictly prohibited.

***7. Server Downtime and Internet Disruption Protocol***

* In the event of a server outage or internet disruption, employees must:
  1. Notify the Senior Engineer immediately.
  2. Continue working offline using locally stored files.
  3. If downtime exceeds one hour, management will evaluate alternative access solutions.
* To ensure reliable connectivity, frequent disruptions should prompt an evaluation of alternative service or network providers.

***8. Cybersecurity Measures***

* Antivirus and firewall protections, including Windows Defender or other approved security software, must be installed and regularly updated on all company devices.
* Multi-factor authentication (MFA) is required for accessing critical systems.
* Employees must participate in annual cybersecurity training.

***9. Hardware/ software Breakdown and Maintenance***

* In case of hardware issues such as problems with PCs, monitors, laptops, or any other devices, third-party services will be utilized to resolve the issue.
* Employees should contact the manufacturer's helpline for assistance or request on-site support if required.
* Consideration should be given to purchasing extended warranties for critical devices that are essential to the organization.

***10. Policy Review and Enforcement***

* This policy will be reviewed annually by the Senior Engineer and Quality Manager.
* Violations of this policy will result in disciplinary actions in accordance with company guidelines.
* Employees are responsible for adhering to this policy and promptly reporting any security concerns.

***11. Acknowledgment***

All employees must read, understand, and sign the Technology Policy Acknowledgment Form to confirm compliance with MME Ltd.’s technology usage standards.