IT POLICY

- We at **menon and menon limited** recognize importance of information and information systems in our business and operations.
- We are committed to ethical use of information and related technologies. Also committed to protect all our information technology assets and systems. And are legally bound by IT Act 2000.
- Any access to information and information systems shall be governed by the information technology policy. This policy would include but not limited to; employees, visitors, guest, business partners, consultants and customers who visit our premise and those who have access of menon and menon Limited's information systems.
- The necessary rules, procedures and guidelines shall be set by information technology procedure manual and related documents that shall be made readily available and accessible to all stake holders.
- All department heads are responsible for implementation of information technology policy in their respective domain and adhere with the rules and procedure defined in this policy.
- We shall continuously endeavour to improve our information security initiative and make it as part of our business action.
- We at menon and menon limited understand value of personal information of all our employees and stake holders. Information technology policy shall ensure mechanisms are adopted to protect individual's privacy.
- This policy will be displayed, made available, accessible, readily available, explained and understood by all the stake holders of this policy.
- We are controlling, monitoring the IT activities as below…

1. INTERNET ACCESS (WIRED & WIRELESS)

1.1 Hardware Firewall: Controlling the 'Gateway' and internet access for different user groups. All the URLs are blocked for access which are not related to our business process and operations. Data downloading limit has been given for different user-groups.

1.2 Wired access has been given to all local desktops. Wi-fi connections are provided for different locations through 'Access Points'.

1.3 No internet connection is to be provided directly to any guest, visitors without proper intimation to Information Center and HR.

1.4 No personal mobiles are allowed to connect to any of company's access control.

1.5 No personal Wi-fi's are allowed to keep open through personal cell phones in the company's premises.

2. STORAGE-MEDIA HANDLING

2.1 Handling storage media from out-side to company and V/v are discouraged.

The USB access of all the desktops are disconnected. In case any requirement same shall be intimated to Information Center. For internal transportation of data-files, internal-shared-could platforms are provided.

2.2 Personnel pen-drives, external HDs and other storage medias are not allowed in the company's premises. Company laptops are to be carried outside factory after taking the approval of reporting authority. Reporting authority shall approve the same with intimation to HR and Security.

2.3 DSC – IT shall compile the list of DSCs available in the company and circulate the list to all control copy holders once in a year. The responsibility and control would be with concerned HOD.

3. EMAIL DOMAIN @menon.in

3.1 MENON.IN is company's authorised domain. No personal communications are allowed through company provided email IDs.

3.2 Company is never responsible for the communications through this domain related to 'personal' usage and registrations in various personal URLs.

3.3 For timely actions over left employee's email IDs, team People Practice shall communicate the same to Information Center. Team Information Center shall change the password and forward the email to next successor for some time and then deactivate the said email ID after taking proper back-up.

4. CONTROL OVER Z REPORTS

4.1 We are encouraging using STD reports available in SAP. Wherever there is no STD reports available and there is a requirement of Statutory, developing customized Z reports after the approval.

4.2 Any 'Z' report is not using by the users for last 6 months, the same Transaction code shall be blocked in SAP by team Information Center.

5. SAP ROLES & AUTHORISATIONS

5.1 For every SAP user has been assigned with required roles and authorizations as per their task in SAP and as per the requirements and proper approvals.

5.2 SAP-User is responsible for the transactions registered with user-ID, hence keep the password un-disclosed and keep changing the password periodically.

5.3 Concurrent user-login is not allowed in SAP system.

5.4 If SAP user is not working continuously for 5 mins, auto log-off facility has been activated. However, user need to log-out immediately after completion of work in SAP system.

5.5 Sharing the SAP Login IDs are not allowed. However, it is allowed to share some IDs in the different shifts with different users. Respective users are responsible for the transactions made as per the attendance in the shifts.

6. DATA SECURITY

Backs-ups are planned and executing as below….

Srn	Particulars	Media	Periodicity
1	SAP DATA	Auto Scheduling through DB13	Daily at 11:45pm
			Weekly
			Monthly
			Quarterly
			Six-Monthly
		DR Server at Data Center – Pune Location	Real Time
		Multiple back-ups on NAS	Auto
2	DESIGN DATA	NAS	Daily auto Scheduled back-up
3	USER DESKTOP DATA	NAS	Twice in a month by concerned user.
4	EMAIL	NAS	One copy is forwarding to Centralised two email IDs – Auto.

- We, hereby, pledge to adhere and abide by the rules and procedures set by this policy. And discharge our roles and responsibilities set forth by menon and menon limited.

Policy Checked by Head – Systems & Strategies Policy Reviewed by Executive Committee member	**Divya Menon** Executive Director

Policy updated on	13/08/2022, 24/08/2022

C:\Users\IT-ADMIN\Desktop\Policies\Policies & Plans\Policy\IT_POLICY_v2.0_2022