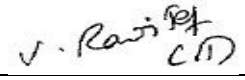
s

Data Protection and Privacy Policy

Responsible Person	IT Manager
Author	IT Manager
Date Effective From	Oct-16-2019
Date Last Amended	Oct-16-2019
Reviewed By	IT – HOD
Approved By	

Data Protection and Privacy

- Account Users must be cautious of the user credentials provided to them for access. MHC Ids, passwords access must not be shared with anybody.
- All MHC data must be classified as 'Confidential' by default and must be protected.
- Data must not be misused for personal gains or handled in an negligent manner which could result in data breaches/identity theft.
- Access to Development, PTST, QA and Production environments must be adequately segregated to reduce the risk of accidental change.
- Must not download sensitive data (classified as confidential) to their desktops/laptops/mobile devices without formal approval from IT/HOD.
- Access to sensitive data internally must be provided only on a 'need-to-know' basis. Access will be provided only for a specified time period with formal approval of IT/HOD.
- Should not forward any of the MHC related information to any of the public domain emails or post sensitive data in blogging sites external to the specific Work Place, without the formal approval from IT/HOD.
- Peer-to-Peer file sharing must not be initiated from MHC supplied laptops hosting sensitive information considering the inherent threat of uncontrolled data theft.

Work Place Security – Dos

- Physical Access to Office is restricted to as per requirement basis. Only authorized team members of the MHC shall have access to the MHC area.
- MHC access shall be controlled using proximity cards.
- All external vendor engineers shall be accompanied by authorized MHC employee/Security. Access of all employees shall be revoked either after separation or during transfer.
- Clear desk policy shall be followed for papers and removable storage media.
- No documents shall be left at printers. Confidential documents should be destroyed securely after use.

- MHC network configuration including the desktops, routers, firewalls, antivirus servers and print servers shall be carried out by authorized personnel from MHC IT team.
- Port configuration in the MHC network workgroup switches (Virtual LANs) shall be carried out by authorized IT personnel as per requirements.
- System privileges shall be granted to users only on a need-to-use basis.
- Users shall have distinct, unique user ids. No group or default id shall be maintained.

Work Place Security – Don'ts

- Desktops/laptops shall not be configured for dial-out connections to Internet or any other untrusted network from MHC LAN.
- Remote access to MHC infrastructure shall be disallowed as a policy. If there is a genuine business case, Remote access shall be allowed only after approval and authorization of IT.
- USB access on desktop/Laptop is not allowed.
- Personal laptops shall not be allowed in MHC networks.
- MHC Documents must not be shared outside MHC Domain.
- Internet access thru MHC network / VPN is strictly prohibited.
- No unauthorized Software's usage is allowed.

Revision History:

Initial	Oct-16-2019