MSC
MicroSave Consulting

Offices across Asia and Africa
www.microsave.net
info@microsave.net

Laptop Management Policy and Procedure

Date: 6 May 2015

Introduction: At MSC, laptops (and related accessories – charger, mouse etc.) are provided to staff and consultants (hereafter referred as 'Users') to facilitate easy access to computing resources at hand at workplace /client sites to be maximally functional and productive. It is user's responsibility therefore to ensure effective usage, timely maintenance and security of the laptops and related accessories.

Policy Statement: The document sets out policy for laptops, the purpose of which is to manage and protect company provided laptops and accessories including management of data risk, if any arising out of usage of laptops.

Scope of Policy: The policy is applicable to all employees and consultants at MSC, who are provided with company owned laptops.

Roles and responsibilities of Users: Laptops are provided for company use only. Users must make all responsible efforts to protect the laptops from theft, damage and data

- Users should not add, modify, delete or upgrade any software from the laptop without any prior information to Administration department.
- Users should get all laptop (hardware / software) problems fixed through and/or under specific intimation to and permission from, the Administration department only.
- Users should take regular backup of data. All sensitive information or document should be password protected.
- Users should not leave the laptops unattended at all times and especially at team meetings, conferences and workshops.
- Users should report Loss / Damage immediately with Administration
- Users should not store client information/ sensitive data on their personal systems / devices. All MSC related data and information must be stored only in official laptops and/or official storage devices as specifically communicated.

Guidelines pertaining to replacement, damage, loss /theft & separation:

Replacement: On completion of three years of the machine, it will be permitted to be retained by the respective user at its minimum assessed value, which will be intimated by the Finance Department. In case the user is not willing to retain the machine, normal procedure for the disposal of the equipment will be followed. On completion of four years of the machine, it will be permitted to be retained by the user at no additional cost (reference: Laptop Replacement Procedure issued dated 20th February 2012)

Damage: In case of any kind of damage to the laptop, the employee should immediately report it to Administration Department who will get the same repaired.

Loss / Theft: Laptops contain sensitive information and pose a major threat to client information and intellectual property in event of theft or loss. Therefore it is required that due care is taken of the entrusted asset. In case the laptop is stolen or lost, the employee shall be liable to pay, per the table below:-

Years	%age of the cost of laptop
0-1	75
Above 1 , up to 2	60
Above 2, up to 3	50
above 3	45

He/ she will be required to register a formal report with the concerned police authorities. Laptop loss should be immediately reported to the Administration Department. The copy of formally registered report should also be submitted. Administration Department will issue a new / available laptop to the user.

Employee may choose the mode of payment in agreement with Finance Department, through any of the following options: a) Single time payment by cheque / cash/ wire transfer; b) payment by post-dated cheques / wire transfer, where by the value is recovered in maximum 3 installments; c) deduction from salary/Fees over a period of time, but not exceeding 3 months.

On Separation: The user should handover the laptop and its accessories in working condition to Admin upon separation. The user should transfer all the company data into the Admin hard disk and remove all access settings before handing it over. It is responsibility of Domain Leaders to ensure that all required data has been properly handed over / saved on KMM repository. If the laptop and accessories are damaged or lost, the same needs to be notified to Admin.

Guidelines pertaining to data secured in laptop:

Since data security and integrity along with laptop (hardware and software) protection is critical to our business and operations, it is also entrusted upon all users that security of data critical to company should not be compromised under any circumstances. Users are deemed custodian of client information, assignment reports, sensitive / confidential data, and indeed any official or business related information.

- Users should secure data on laptop by maintaining monthly back-ups, especially of work related documentation and data created that cannot be retrieved by reinstalling operating system on hard disks issued via Admin to their respective domains.
- Domain Leaders should ensure data back of the team members monthly, as above.
- All documents containing sensitive/client provided/ confidential information should be password protected.
- Users should not expose the laptop to any magnetic fields that could damage the contents of the hard disk as laptops contains a Magnetic Hard Disk.
- On completion of projects, all project related reports and data should be made secure in KMM online repository.
- Users should strive to keep the laptops free from malware by restricting their usage to official requirements only.
- Regular virus scans also needs to be undertaken. IP and data security and integrity must be maintained.