# Employee IT Security Policy for DES

## Purpose:

The purpose of this policy is to set terms and conditions, as well as standards and guidelines, for the acceptable uses of the IT services and assets by the DES employees, contractors and visiting faculty. DES expects employees, contractors and visiting faculty to become familiar with individual and institutional responsibilities to protect its electronic information.

## Scope:

This policy applies to all the users in the DES, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

This IT Security Policy covers the following:

1. IT Assets
2. Password Control
3. Email
4. Internet
5. Antivirus
6. Inventory
7. ERP System
8. CCTV
9. Data Backup

B.M. College of Commerce(Autonomous) Pune-4

OFFICIATING PRINCIPAL
B M College of Commerce
(Autonomous)
Pune - 411 004

## 1. IT Assets

- Employees should handle all the IT assets of DES properly and in a secure manner. This applies to desktops, laptops, printers and other equipment, applications and software, to anyone using those assets.

- Active desktop and laptops must be secured if left unattended.

- Access to assets is forbidden for un-authorized personnel. Granting access to the assets involved in the provision of a service must be done through the approved Service Request Management and Access Management processes.

- Users shall maintain the assets assigned to them in a responsible manner and not cause any damage to them.

- The IT Technical Teams are responsible for maintaining and upgrading configurations. None other users are authorized to change or upgrade the configuration of the IT assets. That includes modifying hardware or installing software.

- Employees should not leave the laptops unattended on the car seats. If it is stolen then the employee will have to pay to the institute with a depreciated value or find a replacement ?

B.M. College of Commerce (Autonomous) Pune-4

OFFICIATING PRINCIPAL
B M College of Commerce
(Autonomous)
Pune - 411 004.

- Special care must be taken for protecting laptops and other portable assets from being stolen. Employees must be aware of extreme temperatures, magnetic fields and falls.

- Whenever possible, encryption technologies should be implemented in portable assets.

- Assets storing sensitive information such as examination question papers must be completely erased in the presence of an Information Security Team member in case of handing over the asset to another employee and discarding or returning the device to the store. Appropriate tools should be used to erase data and format the data.

**2. Password control**

- All laptops and desktops must be protected with a strong password-based access control system.

- Every user must have a separate, private identity for accessing IT network services.

- Each identity must have a strong, private, alphanumeric password to be able to access any service. They should be as least 8 characters long.

- Password should be changed after every 90 days.

B.M. College of Commerce (Autonomous) * Pune-4 *

Bdayekar

OFFICIATING PRINCIPAL
B M College of Commerce
(Autonomous)
Pune - 411 004.

- Sharing of passwords is forbidden. They should not be revealed or exposed to public sight.
- Writing down passwords on notepads or on sticky notes is forbidden.
- Whenever a password is deemed compromised, it must be changed immediately.

**3. Email**

- Henceforth email addresses issued by the organization shall be used for all official communication.
- All the assigned email addresses, mailbox storage and transfer links must be used only for business purposes in the interest of the DES.
- Use of the DES resources for unauthorized advertising, external business, spam, political campaigns, and other uses unrelated to the DES business is strictly forbidden.
- In no way may the email resources be used to reveal confidential or sensitive information from the outside DES. In unavoidable circumstances, confidential data information has to be encrypted or password protected before being sent.
- Using the email resources of the DES for disseminating messages regarded as offensive, racist, obscene or in any way contrary to the law and ethics is absolutely discouraged.

B.M.College of Commerce (Autonomous) Pune-4

BLayekar

OFFICIATING PRINCIPAL
B M College of Commerce
(Autonomous)
Pune - 411 004.

- Outbound messages from all users should have appropriate signatures at the foot of the message.

- Scanning technologies for virus and malware must be in place in client PCs and servers to ensure the maximum protection in the ingoing and outgoing email.

**4. Internet**

- Access to pornographic sites, hacking sites, and other risky sites is strictly forbidden.

- Internet access is mainly for business purpose.

- All internet traffic is guarded by firewall. The employees in no way shall tamper the firewall.

- Attacks like denial of service, spam, phishing, fraud, hacking, distribution of questionable material, infraction of copyrights and others are strictly forbidden.

5. **Antivirus**

- All windows computers and devices with access to the DES network must have an antivirus client installed, with real-time protection.

B.M.College of Commerce (Autonomous) *Pune-4*

OFFICIATING PRINCIPAL
B M College of Commerce
(Autonomous)
Pune - 411 004.

## 6. Inventory

- All items of equipment to be brought under control shall be identified by a serial number affixed to each item.

- Equipment control records shall be maintained for each item of equipment identified by a serial number.

- Periodic physical inventories, at least once annually, shall be taken of all items of equipment placed under serial number control.

## 7. ERP system

- ERP system can be accessed from mobile and PC. Employees will not share login Id or password with anyone.

- The email Id and the contact details provided as input to the ERP system have to be up to date.

- Employees should avoid using the ERP system from any cyber café. In case of unavoidable circumstances, after ERP system is accessed from any cyber café, cache and local copies of any documents should be cleared.

## 8. CCTV

- DES campus is monitored by CCTV for the employees' security. No employee shall tamper it in any way.

B.M. College of Commerce (Autonomous) * Pune-4 *

Bdayeka

OFFICIATING PRINCIPAL
B M College of Commerce
(Autonomous)
Pune - 411 004.

9. **Data Backup**

   - Data Backup is the responsibility of the employee and back up has to be taken on DES approved shared locations. If backup is taken on pendrive or hard disc, it should be encrypted.

10. **Data Privacy Policy**

    - Will be included in next version

11. **Social Media Policy**

    - Will be included in next version

____________________________ hereby agrees to the terms/conditions of this policy.

Sign. Date.

B.M.College of Commerce (Autonomous) * Pune-4 *

OFFICIATING PRINCIPAL
B M College of Commerce
(Autonomous)
Pune - 411 004.