DMC IT Security Policy
Version1.0

1. Table of Contents

Document Change History

Document Distribution List

IT DEPARTMENT	Internal	Database Administrator	Preparer

Intended Audience
IT Staff of IT DEPARTMENT

Conventions used in this document

Abbreviations and Definitions
IT DEPARTMENT

2. Purpose

Security Policy is a Statement of Management Strategy regarding Security of its Information Assets.

3. IT Security Policy

The Policy Statements are grouped under the Following Headings

1. Corporate Policy
2. Information Security Policy
3. Personnel Security Policy
4. Physical & Environmental Security Policy
5. Computer & Networks Security Policy
6. System Administration
7. Network Policy
8. Application Development Policy
9. Business Continuity Planning

3.1.1 Corporate Policy

This Policy lays down the rules for protection of business data and processes corresponding to the threats / risks involved and the value of the assets.

3.1.2 Information Security Policy

The Following requirements must be met

1. All major information assets should have an asset.
2. The owner should classify the information into one of the sensitivity levels depending on costs, Corporate Policy and Business Needs. He /She is responsible for this Information.
3. The owner shall declare who is allowed access to the data.
4. The owner is responsible for this data and shall secure it or have it secured according to its sensitivity.

3.1.2.1 Classification of Information

A classification system is proposed which classes information into four levels. The lowest – 1, is the least sensitive and the highest – 4, is for the most important data / processes. If a system contains data or more than one sensitivity class, it must be classified according that needed for the most confidential data on the system.

3.1.2.1.1 Class -1: Public / Non-Classified Information

Description: Data on these systems could be made public without any implications for the company (i.e., the data is not confidential). Data integrity is not vital. Loss of service due to malicious attacks is an acceptable danger. Examples: Test services without confidential data, certain public information services.
Guidelines on storage: none
Guidelines on transmission: none
Guidelines on destruction: none

3.1.2.1.2 Class -2: Internal Information

Description:
External access to this data is to be prevented, but should this data become public, the consequences are not critical (e.g., the company may be publicly embarrassed). Internal access is selective. Data integrity is important but not vital. Examples of this type of data are internal memos, normal working documents and project/minutes of meeting and internal telephone books.
Guidelines on storage:
Information shall be labelled. i.e., the classification level should be written on documents, media (tapes, diskettes, disks, CD's etc.), electronic messages and files.
IT Systems susceptible to virus attacks should be regularly scanned for viruses. The integrity of systems should be regularly monitored.

Guidelines on transmission:

1. This information shall stay within the company, if it must transit public media (e.g. the Internet), it should be encrypted.
2. Internal data shall not be transferred outside the company unless approved by the IT Department Manager.

Guidelines on destruction: none

3.1.2.1.3 Class -3: Confidential Information

Description:

Data in this class is confidential within the company and protected from external access. If such data were to be accessed by unauthorized persons, it could influence the company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor or cause a major drop in customer confidence. Data integrity is vital. Examples: Salaries, Personnel data, Accounting data, very confidential customer data, sensitive projects, and confidential contracts.

Guideline on storage:

1. Information shall be labelled. i.e., the classification level should be written on documents, media (tapes, diskettes, disks, CD's etc.), electronic messages and files.
2. IT Systems susceptible to virus attacks should be regularly scanned for viruses. The integrity of systems should be regularly monitored. IT Systems shall be configured to protect against unauthorized modification of data and programs.
3. Information shall be kept under lock and key (e.g., documents in locked cabinets, computers in locked rooms).

Guidelines on transmission:

1. Passwords should not be transmitted in clear text (electronically or on paper).

2. This information shall stay within the company, if it must transit public media (e.g. the Internet), it should be encrypted.

Guidelines on destruction:

1. Information shall be securely disposed of when no longer needed (e.g. destruction of old disks and diskettes etc.).

3.1.2.1.4 Class -4: Secret Information

Description:

Unauthorized external or internal access to this data could be critical to the company. Data integrity is vital. The number of people with access to this data should be very small. Very strict rules must be adhered to in the usage of this data. Examples: Information about major pending contracts/reorganization/financial transactions, Strategic Documents etc.

Guideline on storage:

1. Information shall be labelled. i.e., the classification level should be written on documents, media (tapes, diskettes, disks, CD's etc.), electronic messages and files.
2. IT Systems susceptible to virus attacks shall be regularly scanned for viruses. The integrity of systems shall be regularly monitored. IT Systems shall be configured to protect against unauthorized modification of data / programs and shall be audited yearly.
3. Information shall be kept under lock and key (e.g., documents in locked cabinets, computers in locked rooms).
4. Information shall be stored in encrypted format or on removable disks which are physically secured.

Guidelines on transmission:

1. This information shall be encrypted during transmission outside of secure zones.

Guidelines on destruction:

Information shall be securely disposed of when no longer needed (e.g. destruction of old disks and diskettes etc.).

3.1.3 Personnel Security Policy

3.1.3.1 Ethics

Users are not allowed to share accounts or passwords with friends or relatives, run password Checkers on system password files, run network sniffers, break into other accounts, disrupt service, Abuse system resources, misuse email, examine other user's files unless asked to do so by the file Owner, download Soft wares, copy unlicensed software or allow other users to copy unlicensed Software.

3.1.3.2 Password Policy

Adopting a good personal password policy is the most important barrier to unauthorized access in Current systems.

3.1.3.2.1 Content

* Mixture of numbers, capital letters, small letters, punctuation.
* Easy to remember (Should not be written down).
* Easy to type quickly (difficult for an observer).

3.1.3.2.2 Examples

* choose a line or two of a poem, song etc. and use just the first Letters.
* join two small words with a strange character.

3.1.3.2.3 Bad examples

* Name of your spouse, parent, colleague, friend, pet, towns, months, telephone.
* Common dictionary words (French, German, English, Italian...).
* A series of identical numbers/letters.
* Obvious keyboard sequences.
* Any of the above in inverse or with a number before or after.

Guidelines for Passwords

- Don't write down your passwords or disclose via email
- Default password should not be used.
- Don't give your passwords to others
- If Passwords are disclosed on a system change them immediately
- Vendor defined passwords must be changed on systems
- Users should not be able to change other user's passwords, but the system administrator can Change user passwords

3.1.3.3 Network Access Policy

The Following are to be strictly followed for Passwords for Network Access

Minimum Password Length	4
Minimum Password Change Interval	2 Month
Maximum Password Change Interval	4 Weeks
Password History Length	3 Previous Passwords
Lockout Duration	Until Manually Unlocked by System Admin
Lockout threshold	7 Failed Attempts
Lockout Observation Period	1440 minutes

3.1.3.3.2 Network Data Security

Confidential Information

Confidential data transmitted over public networks shall be encrypted

Connection to Networks

- A user may not connect a machine to any network except the corporate LAN.
- Access to external (Public & Private) networks shall occur over a firewall.
- Users may not have modems on their machines
- Users should be aware that conventional email systems often guarantee neither Privacy nor proof of origin or receipt. In many systems the system administrator can read all email.
- Only Class 1 data and information specifically allowed for projects with external Entities may be emailed outside the company.
- Users should be aware of the risks of opening documents with macros, postscript Files, and installing programs received via email.

3.1.3.3.3 Laptops & Portable Computers

Portable Computers allow personnel to be more productive while “on road”. They offer the flexibility As to where one can access information. From the Security Point of View they can create risks of Information disclosure and perhaps form a point of unauthorized point of access to the corporate Network.

Laptop Users should be educated about the risks of Laptop Usage
Password Protection of Office Applications like Word alone will not be a protection for Confidential information.

Removable Hard Disks allows to protect confidential information since it can be easily Removed and stored elsewhere but on the other hand this also makes it easier to steal Information.

So, the following will have to be strictly followed

- Laptops should be prepared and installed by Professional IT Staff
- Windows 7 Professional or above should be used if possible since it give adequate security.
- Users are responsible for the Laptops in their custody
- Automatic screen locking mechanisms and boot passwords should be used where possible
- Virus Scanners must be installed on all laptops.
- Laptops should be carried as hand baggage during travel.
- Class 3 or Class 4 Data should not be carried on laptops unless encrypted.
- Switch off the laptop when not in use
- Never save passwords to Laptops which allow access to corporate systems.
- Do not transmit Class 3 data across insecure networks like GSM, Internet unless encrypted.
- Dial in access Policy will be as per Organization Access Policy.
- Turn off modems when not in use.

3.1.4 Computer & Network Policy

3.1.4.1 System Administration Policy

3.1.4.1.1 Physical Security

- Buildings are classified into the following Zones

    - Zone 1: Areas open to the public.
    - Zone 2: Areas do not open to the public, open to company staff. (Technical Support Room)
    - Zone 3: Protected areas. Access is strictly controlled. Externals are not allowed unless Accompanied egg: - Server Room

- Buildings are to be locked except for access via a reception area
- Public Areas should not have a computer connected to the network.
- Server Rooms must be locked always. Very few People will have access and an access register is to be maintained.

3.1.4.1.2 Backups

- Regular backups should be transferred Offsite regularly.

3.1.4.1.3 Removable Hard Disks

- Removable disks are not to be used within the organization unless absolutely necessary.
- Repair of Hard Disks are not to be performed unless the information has been absolutely Destroyed.

3.1.4.2 Access Control

- All users should be authorized.
- Users should be able to set the privileges of objects belonging to them in their environment.
- Users should be prevented from deleting others user's files in shared directories

3.1.4.3 Logon Policy

- Each user must be identified by a name or number and belong to a group.
- Username and group name structure should be standardized enterprise wide (number of Characters, composition) if possible.
- User and groups must be managed by the System Administrator not by users themselves.
- Each user should have only one account on the system.
- If guest accounts are used, their working environment should be very restricted
- Guest accounts are not allowed.
- Usernames and passwords should not be distributed in the same communication.
- When a user is transferred or terminates employment, his account should be blocked or
- Deleted immediately. Procedures should exist whereby the personnel administration Automatically informs system administrators.
- A screen lock should be activated after 15mins idle time with password protection.
- Users should be informed of actions that violate security. Likewise they must inform their System Administrator if they suspect a security violation.
- If an account is subjected to continuous login failures in short period of time (e.g. 5 attempts),
- Block the account and notify the user.
- If a user enters a bad login name or password, the error message should be the same for both cases. A possible attacker should not be informed if a user account is valid, rather that the combination of account and password is incorrect.

3.1.4.4 Remote Access Servers

- Remote access facility are allowed for selective persons.
- Administrator logins are not to be sent in clear text format.
- Users will be accountable for their actions.
- Remote Servers log file will be audited for unauthorized logins
- Only System Administrator should be able to log into the server locally.
- Remote servers should be in a physically secured room.
- Updates and Configuration Changes are to be performed as per Quality Processes.
- Regular Backup should be taken.

3.1.5 Application Development Policy

Security should be an integral part of new systems. When functional requirements are designed, Security requirements should be formulated corresponding to the sensitivity and availability of data To be handled by the system.

3.1.5.1 General Guidelines

- Separate development and production environments and data.
- Consider security to be an integral part of application development.
- Test data should not contain confidential information.

3.1.6 Business Continuity Planning

Security crisis/disasters
If a serious attack or disaster occurs:

- The IT Department should take charge.
- The concerned machine should be disconnected from the network.
- Document every single action taken, events, evidence found (with time & date).
- Analyze the system: what files changed? What programs/accounts were added or
- modified? If modifications are found, check for these modifications on similar systems.
- Notify management as required.

3.1.7 Enforcement

Users who do not adhere to this policy shall be warned and the corresponding manager informed. Serious Action will be taken against users who continue to ignore warnings.