Information Technology Policy

Department of IT

Table of Contents

Sr. No.	Name of the Content
1	Intent
2	Purpose
3	Information Technology Resources
4	General Information Technology Usage
4.1	Password
4.2	Access Control
4.3	Software Licensing
4.4	Internet and Intranet Usage
4.5	Clear Desk and Clear Screen
5	Email Services and Usage
6	Anti-Malware
7	Technical Vulnerability Management
8	Physical Security
9	Data Backup Policy and Procedure
10	Cyber Security
11	Disaster Recovery

INTENT

Increased protection of information and Information Technology Resources to assure the usability and availability of those resources to all users of DSML. IT is the primary intent of this Policy. The Policy also addresses privacy and usage guidelines for those who access DSML's Information Technology Resources.

PURPOSE

DSML recognizes the vital role information technology plays in effecting organization business as well as the importance of protecting information in all forms. As more information is being used and shared in digital format by DSML's IT resources authorized users, the need for an increased effort to protect the information and the technology resources that support it, is felt by DSML and hence this Policy.

Since a limited amount of personal use of these facilities is permitted by DSML to users, including computers, printers, e-mail, and Internet access, therefore, it is essential that these facilities are used responsibly by users, as any abuse has the potential to disrupt company business and interfere with the work and/or rights of other users. It is therefore expected of all users to exercise responsible and ethical behavior while using DSML's Information Technology facilities.

Information Technology Resources:

Information Technology Resources for purposes of this Policy include, DSML owned or those used under license or contract, Information Technology Resources such as computer hardware, printers, software, e-mail and Internet and intranet access.

a) user:

Anyone who has access to DSML's Information Technology Resources, including but not limited to, all regular employees, temporary employees (contractual and outsourced), probationers, contractors, vendors and suppliers.

b) Scope:

This policy applies to everyone who, has access to DSML's Information Technology Resources and it shall be the responsibility of all users and IT department at the corporate office to ensure that this policy is clearly communicated, understood, and followed by all users.

This Policy also applies to all contracted and outsourced staff and vendors/suppliers providing services to DSML that bring them into contact with DSML's Information Technology resources.

These policies cover the usage of all of the Company's Information Technology and communication resources, whether they are owned or leased by the company or are under the company's possession, custody, or control, including but not limited to :

- All computer-related equipment, including desktop, laptop, wireless computing devices, telecom equipment, networks, biometric devices, printers, and all networks and hardware to which this equipment is connected.
- All applications/services e.g. e-mail, Internet and intranet and other on-line services.

- All software including purchased or licensed business software applications, computer operating systems, firmware, and any other software residing on DSML owned equipment. All intellectual property and other data stored on DSML's Information Technology equipment.
- These policies also apply to all users, whether on Company property or otherwise, connected from remote connections via any networked connection, or using Company equipment.

GENERAL INFORMATION TECHNOLOGY USAGE

a) Passwords

It is imperative that users practice due diligence in controlling access to their systems by protecting their user accounts with passwords which are not easily guessed or deduced. Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the entire corporate network of DSML. As such, all DSML employees (including contract & outsourced employees) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

- Individual password security is the responsibility of each user. Password policy shall ensure that all user accounts are protected by strong passwords and that the strength of the passwords meets the security requirements of the system.
- Passwords are an essential component of DSML's computer and network security systems. To ensure that these systems perform effectively, the users must choose passwords that are difficult to guess. This means that passwords must not be related to your job or personal life. This also means passwords should not be a single word found in the dictionary or some other part of speech.
- To make guessing more difficult, passwords should also be at least eight characters long. To ensure that a compromised password is not misused on a long-term basis, users are encouraged to change passwords (e.g. email, web, desktop, laptop etc.) periodically (at least once every three months).
- Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers, or in other locations where unauthorized persons might discover them. Passwords must not be written down and left in a place where unauthorized persons might discover them.
- Immediately upon assignment of the initial password and in all cases of password "reset" situations, the password must be immediately changed by the user to ensure confidentiality of all information.
- Under no circumstances, the user must share his/her password(s) with other user(s).
- All access codes including user ID passwords, network passwords, PINs etc. shall not be shared with anyone, including personal assistants or secretaries. These shall be treated as sensitive, confidential information.
- The "Remember Password" feature of applications shall not be used.
- Users shall refuse all offers by software to place a cookie on their computer such that they can automatically log on the next time that they visit a particular Internet site.
- First time login to systems/services with administrator created passwords, should force changing of password by the user.
- If the password is shared with support personnel for resolving problems relating to any service, it shall be changed immediately after the support session.

b) Access Control

All DSML computers that are either permanently or temporarily connected to the internal computer networks must have a password-based access control system. Regardless of the network connections, all computers handling confidential information must also employ appropriate password-based access control systems.

- All access control systems must utilize user-IDs, passwords, and privilege restrictions unique to each user. Users are prohibited from logging into any DSML system anonymously.
- Access to the server room is to be restricted and only recognized IT staff or someone with due authorization from the IT Head is permitted to enter the room.

c) Software Licensing

- For all software including like application softwares, computer operating systems, firmware, and any other software must only be purchased or licensed business software applications residing on DSML - owned equipment. Any software which does not have any purchased license must not be used in DSML - owned equipment.
- Use of DSML network resources to illegally distribute or duplicate unauthorized copyrighted or licensed material is prohibited. Users shall not make unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright.

d) Internet and Intranet Usage

- Access to the internet and its resources is provided for the purposes of conducting business on behalf of DSML. Reasonable personal use of the Internet is permitted, according to constraints and conditions set out by the installed Firewall.
- The IT department reserves the right to block access to any Internet resource without any prior notice, in case anyone required access to restricted site, the same may be dealt as special case provided the same is identified as use strictly for official purpose and conducting DSML business. The approval for the same needs to be obtained by the Department Head from the IT Head.
- Similarly, to protect DSML's IT systems from imported viruses, downloading or exchanging screensavers, games, entertainment software or other inappropriate files (for example, video or audio materials for personal use), playing games against opponents or gambling over the internet is not permitted.
- Furthermore, users may not conduct any form of "hacking" or use malicious code to penetrate or attempt to penetrate other computers or to deliberately release viruses or other harmful programs within either the "DSML" network or the internet or bypass security features.

e) Clear Desk and Clear Screen

The Clear Desk and Clear Screen Policy shall communicate the Management's intent to protect information stored in physical and electronic media and minimize risk of unauthorized access.

Following measures may be taken: -

- Computers / computer terminals shall not be left logged-on when unattended and shall be password- protected.
- The Windows Security Lock shall be set to activate when there is no activity for three minutes.
- The Windows Security Lock shall be password protected for reactivation.
- Users shall shut down their machines when they leave for the day.
- There shall be no screen savers set on for the individual's desktops and laptops.

EMAIL SERVICES & USAGE

The e-mail policy helps prevent tarnishing the public image of DSML. When E-mail goes out from DSML, the general public will tend to view that message as an official statement from the organization.

DSML provides electronic mail to staff to enable them to communicate effectively and efficiently with other members of staff, other companies, and partner organizations. When using the Organization's electronic mail facilities all employees shall comply with the email policy. Following points may be adhered to:-

- All authorized users of DSML are provided with an E-mail account, which is either individual to the specific user or generic Email ID and the same is protected with a password which is provided to the individual user. The use of E-mail should be restricted only for the business purpose.
- Email users should be aware that exchange of information with external sites may not be secured with high risks of spam, Trojans, malicious codes etc. Hence the exchange of information should be limited to reliable sites.
- Information must not be transmitted internally or externally which is beyond the bounds of generally accepted standards, values, and ethics. This includes, for example, material which could be considered offensive or discriminatory.
- pornographic or obscene, defamatory or any other material which is otherwise abusive or contains illegal content prohibited by law or regulation of the country or which brings the organization into disrepute. Information is understood to include text, images and is understood to include printing information and sending information via email.
- Security regarding access to the email system is of paramount importance. User identities and personal passwords must not be shared with others. Users should be cautious of providing their email addresses to external parties.
- If it is considered that there has been a breach in the use of the email system, the service of the user will be terminated without any prior information.

ANTI-MALWARE

IT assets must be employed in ways that achieve the business objectives of DSML. IT assets shall be protected in a way that ensures that they are resistant to virus and malware attacks and that all preventive and protective measures shall be used to resist such malware attacks.

DSML shall adopt certain practices to prevent malware problems:

- All workstations whether connected to DSML network, or standalone, must use DSML approved anti-virus and anti-malware software or Equip with End point protection.
- The anti-virus and anti-malware software must not be disabled or bypassed.

- The automatic update frequency of the anti-virus and anti-malware software must not be altered to reduce the frequency of updates.
- Every virus / malware that is not automatically cleaned by the anti-virus and antimalware software constitutes a security incident and must be reported to the IT Team.

TECHNICAL VULNERABILITY

IT systems contain inherent weaknesses that are termed as vulnerabilities. Threats exploit vulnerabilities to cause harm to IT systems. Hence, it is imperative to regularly identify and plug those vulnerabilities and prevent occurrence of security incidents.
The purpose of the Technical Vulnerability Management Policy is to establish rules and principles for identifying and managing vulnerabilities in IT systems of DSML.

PHYSICAL SECURITY

Physical security is an essential part of a security plan. It forms the basis for all other security efforts, including personnel and information security. A balanced security programme must include a solid physical security foundation. A solid physical security foundation protects and preserves information, physical assets, and human assets.

The purpose of the Physical Security Policy is to:

- Establish the rules for granting, control, monitoring, and removal of physical access to DSML office premises.
- to identify sensitive areas within the organization; and
- to define and restrict access to the same.

Following are the policies defined for maintaining Physical Security in DSML.

- Physical access to the server rooms / areas shall be completely controlled and servers shall be kept in the server racks under lock and key.
- Access to the servers shall be restricted only to the IT Team.
- All physical access points (including designated entry / exit points) to the facilities where information systems reside shall be controlled and access shall be granted to individuals after verification of access authorization.
- Physical access to the information systems shall be monitored to detect and respond to physical security incidents.
- Physical protection and guidelines for working in the areas where information systems reside shall be designed and applied.
- Information systems shall be protected from power failure and other disruptions caused by failure in supporting utilities.

DATA BACKUP POLICY AND PROCEDURE

DSML shall adopt and follow well-defined and time-tested plans and procedures, to ensure timely and

reliable backup of its IT assets.
The Backup Policy reiterates the commitment of DSML towards delivering the fastest transition and highest quality of services through the backup arrangement ensuring that its customers, business activities and services do not suffer in any way.

The purpose of this policy is to provide means to:

- Restore the integrity of the computer systems in the event of a hardware/software failure or physical disaster; and
- Provide a measure of protection against human error or the inadvertent deletion of important files.

CYBER SECURITY

Cybersecurity is the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. The field is becoming more important due to increased reliance on computer systems, the Internet and wireless network standards such as Bluetooth and Wi-Fi.

Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes.

To protect from External attack like Backdoor, Denial of service, DDOS attack, phishing, Email Spoofing, IP Address spoofing and MAC Spoofing below should be configured properly in the Network.

- **User account access controls and cryptography** can protect systems files and data, respectively.
- **Firewalls** are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services and block certain kinds of attacks through packet filtering.
- **Intrusion Detection System (IDS)** products are designed to detect network attacks in-progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.
- **Reducing vulnerabilities**

    a) Two factor authentications are a method for mitigating unauthorized access to a system or sensitive information. This increases security as an unauthorized person needs both of these to gain access.
    b) It is possible to reduce an attacker's chances by keeping systems up to date with security patches and updates. The effects of data loss/damage can be reduced by careful backing up and insurance.

- **Hardware protection mechanisms**

    a) Computer case intrusion detection refers to a device, typically a push-button switch, which detects when a computer case is opened. The firmware or BIOS is programmed to show an alert to the operator when the computer is booted up the next time.

b) Drive locks are essentially software tools to encrypt hard drives, making them inaccessible to thieves. Tools exist specifically for encrypting external drives as well.
c) Disabling USB ports is a security option for preventing unauthorized and malicious access to an otherwise secure computer. Infected USB dongles connected to a network from a computer inside the firewall are considered by the magazine Network World as the most common hardware threat facing computer networks.
d) Disconnecting or disabling peripheral devices (like camera, GPS, removable storage etc.), that are not in use.

DISASTER RECOVERY

A disaster is a serious incident that cannot be managed within the scope of DSML's normal working operations. Disaster recovery policy is required to respond to a major incident or disaster by implementing a plan to restore DSML's critical business functions.

The purpose of this policy is to ensure that IT resource investments made by DSML are protected against service interruptions, including large scale disasters, by the development, implementation, and testing of disaster recovery / business continuity plans (DR/BCP). This policy provides a framework for the process of planning, developing, and implementing disaster recovery management for IT Services at DSML.

DSML shall adopt following practices to minimize the impact of disaster: -

- **Control Measures**

Control measures are steps or mechanisms that can reduce or eliminate various threats for organizations. Different types of measures can be included in a disaster recovery plan (DRP). IT disaster recovery control measures can be classified into the following three types:-

- **Preventive measures** – are put in place to identify and reduce risks, as well as restrict the likelihood of preventable disasters.
- **Detective measures** – aim to identify unwanted problems within the IT infrastructure before a more serious event can occur. These can include antivirus software and firewalls, as well as practical approaches, such as fire alarms.
- **Corrective measures** – are put in place to restore a system after a disaster occurs and works to minimize the loss and damage done to the IT infrastructure. This can include backup and disaster recovery services and insurance policies.

Disaster recovery / business resumption plans shall be updated at least annually and following any significant changes to computing or telecommunications environment of DSML.

Employees of DSML shall be trained to execute the disaster recovery plan.