4.3.1
IT Policy

SRI DHARMASTHALA MANJUNATHESHWARA COLLEGE (AUTONOMOUS)

UJIRE-574 240

DAKSHINA KANNADA, KARNATAKA STATE

(Re-Accredited by NAAC at 'A++' Grade)

Ph: 08256-236221,236101(O) Fax: 236220 Mob. : 9148181685

e-mail: principal@sdmcujire.in, sdmcollege@sdmcujire.in, Website: www.sdmcujire.in

4.3.1

I.T. POLICY

Information Technology plays a dominant role in effective classroom communication as well as systemic automation today. Consequently, many associated areas are defined and relevant policies are formulated. Information technology policies articulate the institution's vision, strategy, and principles as they relate to the use of IT resources. The IT policies interpret applicable laws and regulations and ensure that the policies are consistent with legal and contractual requirements. In addition, IT policies specify requirements and standards for the consistent use of IT resources within the institution.

Software Policies

1. The institution shall use only authentic and licensed softwares in all major software requirements.

2. Softwares required for the institution shall be developed in-house by the Software cell.

3. Data and softwares are protected using authentic, paid antivirus package and firewalls.

4. The institution reserves the right to limit, control, restrict and reject access to institutional data and information sharing.

5. Occasionally, verified free software may be used for specific requirements.

6. The hardware as well as software resources shall be managed by a team of trained professionals.

Acceptable use Policy

Since inappropriate use of institutional systems exposes the institution to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of corporate information technology resources for the protection of all parties involved. The scope of this policy includes any and all use of institutional IT resources, including but not limited to the computer systems, email, network, and internet connection. For example, policy outlines things like email use, confidentiality, social media and web browsing, personal use, and how to report security incidents. Acceptable use policy should be the only

one policy which everyone in the organization acknowledges via signature that they have read and understood.

Wireless Network and Guest Access Policy

Wireless access shall be done securely through certain steps to mitigate known risks. Guests/ Authority/ Regulators/ Assessment Bodies access to the institutional network is often necessary for students, customers, consultants, or vendors who are visiting the institution. This may simply take the form of outbound internet access, or the guest may require access to specific resources on the network. Therefore, guest access or other mentioned above to the company network shall be properly controlled. These policies would cover anyone who accesses the network via a wireless connection, including the guest.

Network Security Policy

1. Every institution needs a secure network infrastructure to protect the integrity of its data and mitigate risk of a security incident. The purpose of a specific network infrastructure security policy is to establish the technical guidelines for IT security, and to communicate the controls necessary for a secure network infrastructure.

2. This policy might include specific procedures around device passwords, logs, firewalls, networked hardware's, and security testing.

3. Institutional personnel may not broaden access to institutional data without authorization from the Management. This limitation applies to all means of copying, replicating, or otherwise propagating institutional data. Authorization to access institutional data varies according to its sensitivity. It is important to understand that overall sensitivity of institutional data encompasses not only its confidentiality but also the need for integrity and availability. The need for integrity or trustworthiness of institutional data should be considered and aligned with institutional standards. Unauthorized use/modification of institutional data invites disciplinary/ legal action. The institution is committed to provide quality IT services by constant upgrading of facilities and introduction of latest updated software.

PRINCIPAL
S.D.M COLLEGE
UJIRE - 574240, D.K.

S.D.M. COLLEGE
PIN
574240
UJIRE, D.K.