

INFORMATION TECHNOLOGY POLICY

INFORMATION TECHNOLOGY POLICY

INTRODUCTION

Designing, overseeing, protecting and guaranteeing the best possible use of the information science infrastructure installed on college campuses is the goal of IT coverage. This policy describes the approaches and roles for ensuring the accessibility, privacy and integrity of the data property that the college generates accesses and maintains. Among the information properties covered by the covering are data, fact systems, computers, community devices, mental property, archives and verbally communicated information.

SCOPE

All college staff, students and other users of IT resources—whether individually or as college property—that access and transmit different types of related data are covered by the IT Policy.

OBJECTIVES

The term "users" in this document refers to any individual, student, professor, department, workplace or other entity that is under the management of Dhaanish Ahmed Institute of Technology Campus and needs any of the aforementioned services. To ensure the College IT Systems' availability, dependability, integrity, and optimal performance and that IT sources safeguard the professional e-identity. To ensure that everyone who benefits from the college is responsible for following the procedures controlling the application of this policy record and any other reliant on these rules.

INFORMATION TECHNOLOGY POLICY

SECURITY AND INTEGRITY

PERSONAL USE

The term "users" in this document refers to any individual, student, professor, department, workplace or other entity that is under the management of the Dhaanish Ahmed Institute of Technology Campus and needs any of the aforementioned services. To ensure the College IT Systems' availability, dependability, integrity and optimal performance and that IT sources safeguard the professional e-identity. To ensure that everyone who benefits from the college is responsible for following the procedures controlling the application of this policy record and any other reliant on these rules.

FIREWALL

Additional measures to maintain a secure flow of intranet and internet users within the campus will be handled through the application of Unified Threat Administration.

ANTI-VIRUS AND PROTECTION UPDATES

Regular security updates and antivirus software upgrades are necessary for the protection of computer resources.

POLICY STATEMENT

Users are required to use the management system portal for a number of purposes, including system, internet, radio resources, official website and electronic library resources. The College puts a lot of effort into creating a curriculum that instructs people on how to use IT resources sensibly at all times and for any purpose. College also tries to provide ongoing assistance. Please be aware that the institution will not be responsible for any losses that might happen at that time, under any circumstances.

RESPONSIBILITY

INFORMATION TECHNOLOGY POLICY

Through a centralized registration process at the IT Administration office, all college staff members and students will be able to confirm the authenticity of the information. Nonetheless, the provider is accountable, and the college offers no assurances regarding the information in its whole. The College website is designed and maintained by the IT Administration Office. The following college requirements cover the essential updates and maintenance for hardware and software.

OPERATING ASPECTS

Institutional leaders are accountable for adhering to all college policies regarding the use of information resources while keeping the institution's vision and aim in mind. At the college level, the Chief Administrative Officer works with the IT administrators at each college to coordinate a variety of tasks relating to IT policy compliance. Individual users' activities on college servers using their assigned IP addresses and "username/password" pairs are wholly their own.

IMPLEMENTATION

A committee known as the IT Administration Committee is responsible for implementing information and technology policies. The College will enact the required rules in order to carry out this directive.

REVIEW AND MONITORING

At least every two years, policy documents must be reviewed and revised. A committee led by college administrators, heads of institutions, academics in general administration and other individuals is reviewing this policy statement.