Contents

1 Cyber Security Policy

The Bapatla Engineering college has a complex and resource rich information technology environment upon which there is increasing reliance to provide mission-critical academic, instructional and administrative functions. Safeguarding the institution's computing assets in the face of growing security threats is a significant challenge requiring a strong, persistent, and coordinated program that leverages widely accepted, effective security practices appropriate for the higher education environment. Cybersecurity policy seeks to provide guidance for the protection of critical data, IT assets, and infrastructure at the institute level.

1.1 Acceptable Use Policy

This policy of the college views administrative data, third party proprietary information, and college information systems as critical business assets. Misuse or damage of administrative data, third party proprietary information, or college information systems may be as costly to the college as misuse or damage of physical property. Hence, Students and college employees are responsible for the protection and proper use of college administrative data, third party proprietary information, and information systems according to the policy provisions set forth below.

1.1.1 Acceptable Use Policy for Students

The following activities are prohibited:

- Transmitting unsolicited messages which constitute obscenity, harassment or threats;
- Communicating any information concerning any password, identifying code, personal identification number or other confidential information without the permission of the controlling authority of the computer facility to which it belongs;
- Gaining or attempting to gain unauthorized access to, or making unauthorized use of, a computer facility or software. This includes creating, copying, modifying, executing or retransmitting any computer program or instructions with the intent to gain unauthorized access to, or make unauthorized use, of a computer facility or software.
- Creating, copying, modifying, executing or retransmitting any computer program or instructions intended to obscure the true identity of the sender of electronic mail or electronic messages,

collectively referred to as "messages," including, but not limited to, forgery of messages and/or alteration of system and/or user data used to identify the sender of messages;

- Accessing or intentionally destroying software in a computer facility without the permission of the owner of such software or the controlling authority of the facility;
- Making unauthorized copies of licensed software;
- Communicating any credit card number or other financial account number, or any social security number without the permission of its owner;
- Effecting or receiving unauthorized electronic transfer of funds;
- Using the computer facilities in a manner inconsistent with the college's license agreements or contractual obligations to suppliers or with any published policy;
- Using college information systems for commercial gain;
- Illegally using copyrighted software and materials, storing such materials on college information systems, or transmitting such materials over the college network facilities;
- Knowingly engaging in any activity harmful to the information systems (e.g., creating or propagating viruses, overloading networks with excessive data, instituting or promulgating chain letters, or instigating unauthorized mass postings of any type);
- Circumventing or subverting any system or network security measures.

1.1.2 Acceptable Use Policy for Faculty and Staff

- Restricted college administrative data and third-party proprietary information (e.g., licensed software and designated portions of vendor contracts) in the custody of college staff members shall be used only for official college business and as necessary for the performance of assigned duties. Restricted college information includes student records that are confidential, personnel records, and other data to which limited access is subject to prior administrative approval.
- college administrative data or third-party proprietary information shall not be altered or changed in any way except as authorized in the appropriate performance of assigned duties.

- college administrative data or third-party proprietary information shall not be divulged to anyone unless their relationship with the college as an employee, customer, vendor, or contracted temporary employee warrants disclosure and is authorized or required by law and college policy.
- Unless publicly available, college administrative data shall only be accessed by staff members who are specifically authorized to do so.
- college information systems shall not be used for personal economic benefit or for political advocacy. Occasional use (e.g., email, web) of college information systems for personal use is acceptable if it does not interfere with a staff member's job performance.
- Any user IDs and passwords assigned to a faculty or staff member shall be used only by that faculty or staff member and shall not be shared with others.
- The college strictly prohibits illegal use of copyrighted software and materials, the storage of such software and materials on college information systems, and the transmission of such software and materials over the college network facilities.
- The college is providing staff members with access to shared resources. Staff members shall not knowingly engage in any activity harmful to the college's information systems, administrative data, or third-party proprietary information. (e.g., creating or propagating viruses, overloading networks with excessive data, instituting or promulgating chain letters, or instigating unauthorized mass postings of any type).
- The college information systems shall not be used to engage in any activity prohibited by college policies, or by state or central law.
- college staff members shall not circumvent or subvert any college system or network security measures. They shall not use college email services to harass or intimidate another person. They shall not send email using or impersonating someone else's user ID or password.
- The college does not routinely inspect, monitor, or disclose electronic mail. However, electronic messages are written records and may be subject to disclosure under the Freedom of Information Act, legal process, or college review upon receipt of a credible allegation of misconduct. The college will investigate and may pursue appropriate internal or external civil or criminal proceedings when misuse of

college administrative data, third party proprietary information, or college computing resources is suspected.

- Failure to comply with any of the above stated policies may result in a staff member being disciplined or terminated from his or her position, in accordance with general employment policies and procedures that apply to respective categories of employees.
- This policy does not affect the duties, powers and responsibilities of the Management.

1.2 System and Data Classification Policy and Procedures

1.2.1 Purpose

This document defines the college's system and data classification scheme and established procedures for protecting critical IT systems and sensitive college data processed, received, sent, or maintained by or on behalf of the college.

1.2.2 IT System Classification

Systems of the college are classified as either critical or non-critical. The college has identified systems that are critical based on their role in supporting the colleges primary mission: teaching, research, and public service. Additionally, any system identified as essential during an emergency event is also classified as critical. Critical IT systems require a higher degree of protection and are, therefore, subject to stricter controls for access management, logging and monitoring, and disaster recovery planning.

1.2.3 Data Classification

Data owned, used, created or maintained by the college is classified into the following three categories:

- Public
- Internal Use Only
- Sensitive

Departments should carefully evaluate the appropriate data classification category for their information. When provided in this policy, examples are illustrative only, and serve as identification of implementation practices rather than specific requirements.

- Public data:

  Public data is information that may or must be open to the general public. It is defined as information with no existing local, national or international legal restrictions on access or usage. By way of illustration only, some examples of Public Data include:

  - Publicly posted press releases
  - Publicly posted schedules of classes
  - Public announcements, advertisements, directory information, and other freely available data on college websites

- Internal use data:

  Internal Use Data is information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Internal Use Data is information that is restricted to members of the college community who have a legitimate purpose for accessing such data. By way of illustration only, some examples of Internal Use Data include:

  - Employment or personnel data
  - Budget reports, internal memos, or other business related data
  - Project management documents
  - Departmental operating procedures
  - Performance evaluations

  Internal Use Data:

  - Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure.
  - Must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
  - Must not be posted on any public website.
  - Must be destroyed when no longer needed subject. Electronic storage media shall be sanitized appropriately by overwriting or degaussing prior to disposal. Disposal of electronic equipment must be performed so as to avoid any Dumpster diving attacks.

- Sensitive data:

  Sensitive data is information protected by statutes, regulations, or contractual language. Managers may also designate data as Confidential. Confidential Data may be disclosed to individuals on a need-to-know basis only. Disclosure to parties outside the college should be authorized by executive. By way of illustration, some examples of sensitive data include:

  - Aadhar card numbers, driving license numbers, credit/debit card numbers, passport numbers
  - Student personal and academic records
  - Personally identifiable financial information
  - Proprietary vendor information
  - Health records
  - Employee Relations Cases or information related to disciplinary actions
  - System account credentials
  - Records related to internet activity including, but not necessarily limited to, Domain Name Service (DNS) records, netflow records, internet search histories

  Rules for Managing Sensitive Data

  - Sensitive data may only be collected, maintained, used, or disseminated as necessary to accomplish a proper academic or business purpose of the college or as required by law.
  - Individuals have the right to inspect and challenge, correct, or explain their personal information.
  - Sending and/or Receiving Sensitive Data in Electronic or Physical Form. The following restrictions apply both to internal data transmissions (such as sharing files with another college employee) as well as transmissions to outside parties.
    * Sensitive data sent and/or received electronically must be secured using encryption technology, a secure web transfer, or the Secure File Transfer Protocol.
    * Routine exchange of sensitive data with a third party requires a signed interoperability agreement or other contract describing which party is responsible for securing sensitive data in transit and how the data will be secured, and any specific confidentiality obligations.

    * For any other release of sensitive data by the college to a third party the sender must ensure that the third party is aware of the confidentiality obligations applicable.
    * Sensitive data sent in physical form, such as through the post office or interdepartmental mail, must be secured in a sealed envelope or similar method and marked confidential.
    * Faxing sensitive data is permitted provided that the recipient is notified in advance and is available to retrieve the fax immediately following transmission or able to secure it upon receipt (ie receiving a fax in an office that is only accessible by the recipient). Individuals receiving faxed documents with sensitive data are responsible for securing the document after receipt.

Storing Sensitive Data

- Sensitive data should be kept on college administered servers. If sensitive data must be stored on personal or college-owned devices, including but not limited to laptops, personal computers, CDs, flash or thumb drives, cell phones, and/or personal computing devices (i.e. smartphones, tablets, etc...), the sensitive data must be encrypted and said devices must be password protected.
- Sensitive data saved in non-electronic form (i.e. paper or a white board) must be protected from unauthorized access when left unattended and destroyed when it is no longer needed. For example, papers with sensitive data cannot be left on an unattended desk but instead must be filed in a locked cabinet or a locked office.
- Destruction of Electronic Media Containing Sensitive Data: Electronic media including computers jump or flash drives, CD/DVDs, or servers on which sensitive data has been stored must be disposed of carefully so as to avoid Dumpster diving attacks.