# Information Systems Security Policy

## 1] Policy Statement

I. Any Information is a critical asset of Parvatibai Chowgule College of Arts & Science. Accurate, timely, relevant, and properly protected information is essential to the success of the College's academic and administrative activities. The College is committed to ensuring all accesses to, uses of, and processing of College information is performed in a secure manner.

II. Technological Information Systems play a major role in supporting the day-to-day activities of the College. These Information Systems include but are not limited to all Infrastructure, networks, hardware, and software, which are used to manipulate, process, transport or store Information owned by the College.

III. The Policy provides a framework in which security threats to College Information Systems can be identified and managed on a risk basis and establishes terms of reference, which are to ensure uniform implementation of Information security controls throughout the College.

IV. The College recognizes that failure to implement adequate Information security controls could potentially lead to:
- Financial loss
- Irretrievable loss of Important College Data
- Damage to the reputation of the College
- Legal consequences

Therefore measures must be in place, which will minimize the risk to the College from unauthorized modification, destruction or disclosure of data, whether accidental or deliberate. This can only be achieved if all staff and students observe the highest standards of ethical, personal and professional conduct. Effective security is achieved by working with a proper discipline, in compliance with legislation and College policies, and by adherence to approved College Codes of Practice

V. The Information Systems Security Policy and supporting policies apply to all staff and students of the College and all other users authorized by the College.

The Information Systems Security Policy and supporting policies relate to use of:

- All College networks connected to the College Backbone

- All College-owned/leased/rented and on-loan facilities.

• To all private systems, owned/leased/rented/on-loan, when connected to the College network directly, or indirectly.

• To all College-owned/licensed data/programs, on College and on private systems.

VI. The objectives of the Information Systems Security Policy and supporting policies are to:

• Ensure that information is created used and maintained in a secure environment.

• Ensure that all of the College's computing facilities, programs, data, network and equipment are adequately protected against loss, misuse or abuse.

• Ensure that all users are aware of and fully comply with the Policy Statement and the relevant supporting policies and procedures.

• Ensure that all users are aware of and fully comply with the relevant Information Technology (Amendment) Act, 2008 legislation.

• Create awareness that appropriate security measures must be implemented as part of the effective operation and support of Information Security.

• Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.

# 2] IT Management Roles and Responsibilities

**I. The Committee To Oversee Cyber Policy (COCP)**

The COCP is responsible for approving the IT Security Policy, distributing the policy to all heads of department and for supporting the IT security officer in enforcement of the policies where necessary.

Committee members include:

i) Principal

ii) Vice-Principals

iii) Head, department of computer science

iv) IT security officer

**II. The IT Security Officer**

The IT Security Officer is responsible for:

- Reviewing and updating the Security policy and supporting policies and procedures.
- The promotion of the policy throughout College.
- Periodical assessments of security controls as outlined in the Security Policy and procedures.
- Investigating Security Incidents as they arise.
- Maintaining Records of Security Incidents. These records will be stored for statistical purposes.
- Reporting to the Principal, Heads of department and other appropriate persons on the status of security controls within the College.

**III. Information Systems Users**

It is the responsibility of each individual Information Systems user to ensure his/her understanding of and compliance with this Policy and the associated Codes of Practice.

All individuals are responsible for the security of College Information Systems assigned to them. This includes but is not limited to infrastructure, networks, hardware and software. Users must ensure that any access to these assets, which they grant to others, is for College use only, is not excessive and is maintained in an appropriate manner

**IV. Purchasing, Commissioning, Developing an Information System**

All individuals who purchase, commission or develop an Information System for the College are obliged to ensure that this system conforms to necessary security standards as defined in this Information Security Policy and supporting policies.

Individuals intending to collect, store or distribute data via an Information System must ensure that they conform to College defined policies and all relevant legislation.

## V. Reporting of Security Incidents

All suspected information security incidents must be reported as quickly as possible through the appropriate channels. All College staff and students have a duty to report information security violations and problems to the IT Security Officer on a timely basis so that prompt remedial action may be taken. Records describing all reported information security problems and violations will be created.

Incidents can be reported via:

(i) Email (itofficer@chowgules.ac.in)

(ii) Appointment with IT security officer (Any time)

(iii) Complain Box in Lab 3

## VI. Compliance with Legislation

The College has an obligation to abide by legislation of India The relevant acts, which apply in Indian law to Information Systems Security, include:

- Information Technology (Amendment) Act, 2008.
- The Information Technology Act, 2000.

# 3] Breaches of Security

## I. Monitoring

The Information Systems Services department will monitor network activity, reports from the OIT and take action/make recommendations consistent with maintaining the security of College information systems.

## II. Incident Reporting

Any individual suspecting that there has been, or is likely to be, a breach of information systems security should inform the IT Security Officer or the OIT help desk immediately who will advise the College on what action should be taken.

## III. Enforcement

The Principal or committee has the authority to invoke the appropriate College disciplinary procedures to protect the College against breaches of security.

In the event of a suspected or actual breach of security, the committee or the IT Security Officer may, after consultation with the Principal make inaccessible/remove any unsafe user accounts, data and/or programs on the system from the network.

## IV. Action At Institutional Level

In the event of a suspected or actual breach of security,

- The IT Security Officer will report to Principal
- Unsafe users college accounts would be disabled
- Committee verifies report and recommends action plan to principal
- Action would be notified to respective Mentor/Parent/student
- Immediate suspension from college
- Fine would be charged 5 times the replacement cost of the stolen/damaged asset amount
- Committee will go with Legal implication if necessary

## V. Legal Implications

Any breach of security of an Information System could lead to loss of security of personal information. This would be an infringement of Information Technology (Amendment) Act, 2008 and could lead to civil or criminal proceedings. It is vital, therefore, that users of the Colleges

Information Systems must comply, not only with this policy, but also with the College's Data Protection policy.

## VI. Disciplinary Procedures

Failure of an individual student or member of staff to comply with this policy may lead to the instigation of the relevant disciplinary procedures and, in certain circumstances, legal action may be taken.

## Procedure For Lodging Cyber Crime Complaints

### 1] Contact:

# GOA POLICE, Margao

| | |
|---|---|
| Police Control Room, Margao | 2714450 , 2714450 |
| Police Exchange, Margao | 2700142/143<br>2712816 |

### 2] Send Email To Following Email IDs:

| | |
|---|---|
| Director General of Police, Goa | dgpgoa [ at ] goapolice.gov.in |
| Inspector General of Police Goa | igpgoa [ at ] goapolice.gov.in |
| Superintendent of Police North Goa | spn-pol.goa [ at ] nic.in |
| Superintendent of Police South Goa | sps-pol.goa [at ] nic.in |
| General e-mail | goapol [ at ] bsnl.in |

# REFERENCE

According to Goa Police , we follow section 55, 65, 66 of Information Technology Amendment Act 2008 which are given below for your reference :

**55. Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings.-**
No order of the Central Government appointing any person as the Chairperson or the Member of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.
**In section 55 of the principal Act, for the words "Presiding Officer", the words"Chairperson or the Member" shall be substituted**

**65. Tampering with Computer Source Documents.-**
Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to 2 lakh rupees, or with both.

***Explanation*** **-** For the purposes of this section, "Computer Source Code" means the listing of programme, Computer Commands, Design and layout and program analysis of computer resource in any form.

**66. If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.**
*Explanation.*—For the purposes of this section,—
(*a*) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code;
(*b*) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code.

**66A. Any person who sends, by means of a computer resource or a communication device,—**
(*a*) any information that is grossly offensive or has menacing character; or
(*b*) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device,
(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,

shall be punishable with imprisonment for a term which may extend to three years and with fine.

*'Explanation.*— For the purpose of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, images, audio, video and any other electronic record, which may be transmitted with the message.

**66B. Whoever dishonestly received or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.**

**66C. Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.**

**66D. Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupee.**

**66E. Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.**

*Explanation.*— For the purposes of this section—

(*a*) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

(*b*) "capture", with respect to an image, means to videotape, photograph, film or record by any means;

(*c*) "private area" means the naked or undergarment clad genitals, public area, buttocks or female breast:

(*d*) "publishes" means reproduction in the printed or electronic form and making it available for public;

(*e*) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that—

(*i*) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(*ii*) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

**66F. (*1*) Whoever,—**
**(*A*) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by—**

*(i)* denying or cause the denial of access to any person authorized to access computer resource;

(*ii*) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

*(ii)* introducing or causing to introduce any computer contaminant;

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or discruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

**(*B*) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct btains** access to information, data or computer database that is restriced for reasons for the security of the State or foreign relations, or any restrictued information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the secrity of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,commits the offence of cyber terrorism.

**(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with**

*(i)* imprisonment which may extend to imprisonment for life.'.

**In section 43 of the principal Act,—**

(a) in the marginal heading, for the word "Penalty", the words "Penalty and Compensation" shall be substituted;

(b) in clause

(a), after the words "computer network", the words "or computer resoruce" shall be inserted;

(c) after clause (h), the following clauses shall be inserted, namely:—

"(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(j) steel, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;";

(d) for the portion begining with the words "he shall be liable to pay damages" and ending with the words "persons so affected" the following shall be substituted,

namely:—
“he shall be liable to pay damages by way of compensation to the person so affected”;
(e) in the Explanation,
after clause (iv), the following clause shall be inserted, namely:—
‘(v) “computer source code” means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.”.

**22. After section 43 of the principal Act, the following section shall be inserted, namely:—**

‘43A. Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation.—For the purposes of this section,—
(i) “body corporate” means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(ii) “reasonable security practices and procedures” means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

(iii) “sensitive personal data or information” means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.’.