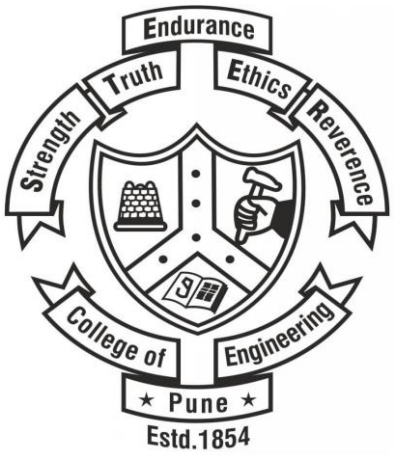

College of Engineering Pune

(COEP)

(An Autonomous Institute of Govt. of Maharashtra)

Shivajinagar, Pune-411005

Cyber Security Policy Document

(Release: April 2020, Version 1.0)

Index

1. Preamble

College of Engineering Pune (COEP) is an autonomous institute of the Government of Maharashtra (Est.1854). All on-campus stakeholders of our institute are empowered with state-of-art ICT facilities in terms of uninterrupted access to internet on their device (desktop, laptop, cell phones) through wired and wireless connectivity with sufficient bandwidth. In the cyberspace the information is exchanged between user, software and services throughout the world, with the support of Information and Communication Technology (ICT) devices and networks. The aim behind framing this cyber security policy document is to safeguard the information and infrastructure in cyberspace. This policy document is also helpful for building proficiencies to avoid and respond to cyber threats, minimize vulnerabilities and loss from cyber events using a combination of institutional structures, technology, people, processes and cooperation.

2. Objectives

1) To form a secure cyber environment in the institute, create sufficient faith & assurance in IT systems and enhance adoption of IT.
2) To identify and minimize the impact of compromised information assets such as data misuse and misuse of other devices like mobile, computers, networks & applications.
3) To create organizational model for information security and supporting actions for compliance to legal, ethical global security standards like NIST, GDPR, HIPAA, FERPA and other best practices
4) To create a private and secure culture through responsible user conduct & actions by an operative communication

5) To provide effective mechanisms which will respond to queries and complaints, that are related to real or perceived cyber security risks such as phishing, malware and ransom-ware

3. Scope

The scope of this policy framework includes the entire institute, including all the departments, all administrative, academic, research units, and the entire networking environment (including remote and mobile users) of the institute. The Policy is intended to guide effective protection of all systems infrastructure, applications, services, databases and information assets. It will also report the challenging requirements raised by security of cyberspace at large.

4. General Policies:

All College Students, Faculty / Staff, Alumni and Guests, all collectively referred to as “Users”.

4.1 COEP's IT Infrastructure

College of Engineering Pune (COEP) have its own powerful and well maintained IT infrastructure which facilitates the students, research scholars and the faculty to do their work efficiently. This infrastructure includes:

1. Computer Hardware
2. Computer Software
3. Data Management Technology
4. Networking Technology
5. Information Technology Services

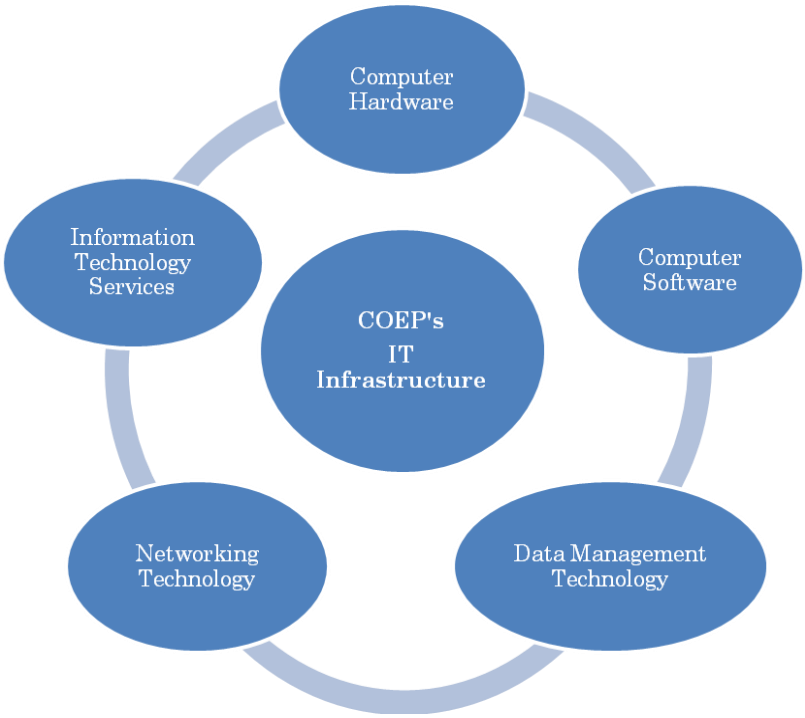

Figure 1: IT Infrastructure Components

4.2 Access to IT Resources policy

IT resource allocation is prepared for the purpose of academic and related activities. It can also be used for special purposes and it has to obtain express and explicit consent from the Data Centre.

The Institute prohibits its users from gaining or enabling unauthorized access to forbidden IT resources on the Institute network. Any such attempt will not only be the violation of Institute Policy but may also violate national and international cyber laws, provisions under The Information Technology Act of India and infringe the principals of National Cyber Security Policy and it is subject to both civil and criminal responsibility.

However, the Institute reserves all the rights to access and analyze the IT resource and Information for any legal and/ or institutionally provisioned operation, on its own or through its affiliates.

a) Non-transferable Identities

All user identities on the Institute network are non-transferable and shall not be shared or used by any other user. Any such known or unknown usage shall constitute violation of the Institute's policy.

b) Proprietary nature of information

All the information belonging to other users (such as data, programs or any other digital material, passwords etc.) shall remain proprietary in nature and without obtaining specific permissions form respective users, other users shall not use or possess or share any such information in its original or modified form.

c) Use of Individual owned IT Resources

It is not permitted to connect any personal active networking devices such as network switches, hubs, wireless access points, routers etc. to the institute's network. All IP addresses will be allocated and administered only by Data Centre. In the interest of better safety of user(s), appropriate policy compliance or due to legal proceeding, all or part of computing devices owned by the users, may be monitored and/ or analyzed or audited with or without any prior notice by the institute or through third-party service providers.

4.3 Policy of legitimate Use of IT resources

The users of IT infrastructure of the Institute are also by default governed by the prevailing laws of the land. Further, current policy document broadly indicates Institute's commitment towards observing such security mandates and legal bindings. The 'users' are therefore also advised to be aware and remain compliant to various legal obligations, licenses, contracts and prevailing IT Act of India, National Cyber Security Policy, etc.

a) Prohibited Use

The Institute prohibits its users from sending, viewing or downloading any kind of message or material which will violate the applicable law or

Institute policy i.e. kind of threatening, fraudulent, distressing, offensive (i.e., pornographic). Therefore, user's inhibitive discretion is solicited where category of certain content could be doubtful e.g. when such content is received through e-Mail etc.

As a generalized policy, any contribution towards the destruction or distortion of congenial academic or work environment is prohibited.

b) Caution regarding Copyrights and Licenses

Users must not violate any IPR and copyright law(s), and licensing policies as associated with copyrighted materials and software. Any unlawful file-sharing, use of any form of illegal or pirated or un-licensed software, on the Institute's IT resources (including individually owned IT resource being used under Institutional IT privileges) is strictly prohibited and any such act shall constitute a violation of the Institute's policy.

4.4 Software and Hardware Usage Policy

a) The IT Users are instructed to install/download only genuine, licensed softwares /tools /patches / libraries on their desktop computer/workstation/laptop or any other computing device.

b) New software can be downloaded and installed with the prior permission from the respective facility in-charges. Unlicensed software should not be installed on COEP amenities, or on any individual machines connected to the COEP network and doing it is rigorously not allowed.

c) Downloading of torrent software, pirated softwares, copyrighted movies, songs, entertainment content through college network is strictly prohibited.

d) Transfer of copyrighted materials to or from the COEP systems without prior permission of the owner is a violation of international law. In addition, use of the internet for profitable gain from an educational site is strictly prohibited. If this is done, it will be the responsibility of that particular user.

e) Downloading of copyrighted movies /books/games via torrent's or other means is traceable and students are warned that on receipt of any complaints appropriate disciplinary action will be taken by the institute's I-CSC disciplinary sub-committee.

f) Use of institute laboratories or institute facilities for playing games is strictly not allowed.

g) It is the responsibility of all the users to take necessary care of IT equipment, and they are also expected to bring to the notice to the staff on duty or to the facility in-charge for any malfunction. Users are not allowed to transfer, repair, reconfigure, change, or attach external devices to the systems.

h) The Data Centre is responsible for monitoring College‘s IT resources to manage day-to-day information security activities. The Data Centre may decide to audit the systems to identify and mitigate risks, or to make in accessible/remove any unsafe usernames, data and/or programs on any College owned Machine.

4.5 Internet Usage Policy

As per the requirement of IT Act and National Cyber security guidelines every internet access using COEP's IT resources to specific users, data center will maintain three months log. Internet access from the wired and wireless (wi-fi) will only be accessible from the designated proxy servers. All accesses will be logged with the URL, access time, uid of the user and registered IP and MAC address of the devices (desktop, laptop, mobile, tablets etc). The log will be maintained for three months. The data usage and download limits will be decided by the data center to control the access to internet within the institute.

The data center in-charge is accountable, to install proper firewall and impose security measures so that the access is restricted to the specific server only. As, internet access will be available through NAT/PAT at the firewall and all the

external accesses will be logged at the firewall, it will include the time of access and the NAT/PAT mappings. So in all such cases, the COEP network is completely protected from external accesses.

4.6 Email Account Usage Policy

a) All the users of COEP including faculty, staff and students are provided an official email-id in the domain www.outlook.com/coep.ac.in. The use of shared email accounts for any purpose is not allowed. Any special accounts, if need to be set up for conferences, workshops, Symposiums, STTPs, FDPs etc and other valid reasons as determined by the institute authorities, must have a single responsible user.

b) According to the institute's policy all users are expected to use institute's email-id in all official correspondence. Use of COEP's email account other than official purpose will be against the institute's policy. Email account users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the institute or any department or unit of the institute unless appropriately authorized to do so.

c) The authenticity of any email that is accepted cannot be guaranteed by the mail transfer protocol. All users are advised to cross check in case of doubt or use digitally signed emails. In case emails are digitally signed, the authenticity is certified by the certificate provider and it is the user's responsibility to verify the certificates.

d) Once a faculty is relieved from institute then his/her email-id should be disabled/blocked within a period of one month from date of reliving. Passing out student willing to continue COEP's email-id should submit an application to continue to use the email-id in prescribed format available on COEP Website. Those who will be failing to do so his/her email-id will be disabled/blocked on 30th June of the academic year without any further notice.

e) Password of email accounts should be kept secure. Sharing of password with others is strictly prohibited. It has been suggested/recommended to change the password of email-id periodically or based on the threat to compromise the email account. It case of resetting the password of the email account, user should submit an application in prescribed format (available on COEP Website) to data center through proper channel.

f) All email transactions logs (both incoming and outgoing) are maintained for three months after which they are automatically deleted. Again, the administrators have access to these logs. Automated programs may be run by administrators to generate performance statistics and/or to train tools for spam and misuse detection. The administrators follow the policy of never examining the contents of the log to determine who sent mails to whom unless they are required to do so as a part of investigation of misdemeanor, or for debugging mail problems.

g) All the users should follow the ethics of using email account and should not misuse the same which will be against the institute's policy. There are a few scenarios of such misuse of emails given below but not limited to:

- Violations of copyright law
- Sending harassing/abusing emails
- Intentionally forwarding or originating hoaxes, scams, spam or other types of fraudulent messages through emails
- It is also prohibited to send emails or messages masquerading as another person or to hide the sender's identity
- Intentionally sending viruses, worms or any other "malwares" through emails
- Sending unsolicited mass mailings without the consent of all addressees, unless authorized on behalf of the institute by an competent authority
- Any commercial use for personal profit through emails

5. Terms of Use of Social Media

By agreeing to abide by the terms of use of various online/ social media forums, the users are expected to adhere with the norms as prescribed by respective social networking websites, mailing lists, chat rooms, blogs, etc.

5.1 Staff

All employees should rethink, whenever they are posting on their social media accounts about the institute. The institute does not and will not monitor individuals' accounts. However, if an issue is raised regarding the content posted on a staff members' social media account and the post is considered to be misbehavior, the institute has the right to demand the removal of content. Severe breaches which includes, but not restricted to, harassment or bullying of colleagues and the misuse of confidential information may constitute gross misconduct and may lead to disciplinary action prescribed by the I-CSC disciplinary sub-committee.

5.2 Student

Social media can be a positive tool for any student for discussing and researching academics but it is essential to think carefully to post content and maintain account security in order to mitigate the associated risks. Posting offensive, inappropriate contents related to the institute or sharing any unlawful material can have a number of serious consequences, including, but not restricted to:

- expressively impacting on an individual's academic prospects
- damaging the institute's reputation
- legal action on the student

As per the institute's policy, students must not:

- break others' privacy by sharing sensitive or personal information
- By cheating assume the identity of another
- post or support content which harasses or bullies fellow students
- post or support content intended to provoke violence or hatred

- post or support offensive content relating to an individual's sex, sexual orientation, religion or belief, race, pregnancy/maternity, marriage/civil partnership, gender reassignment, disability or age
- post or support content which harms, or has the possibility to harm, the institute's relationships with the local community or other bodies or organizations
- use the College logo or any other College images or icons on personal social media sites

Disciplinary action may be taken, if anyone fails to act in line with the above terms.

6. Website data uploading

The data on the official website of the institute website (www.coep.org.in) is handled by the institute's Web-team duly constituted by head of the institute time to time. All the website data operations such as creation / removal of any type of web content is carried out by the authorized team members only. Any request to upload any web page/ content on the institute's website will be permitted after screening the genuineness of the purpose and appropriateness of the content by the web team and with due permission of the in-charge data center. As long as adequate support and resources are available, faculty may host web pages for "affiliated" professional organizations on the institute's website. Prior approval from the competent administrative authority must be obtained for hosting such pages.

7. Policy violation and investigation

Users are solely responsible for understanding and following this cyber security policy. Any violation of any part of this policy and/or any misuse of any part of the IT infrastructure by any user or using any account owned by the user is solely the responsibility of the user. Any liability or legal action arising out of any such violation/misuse will solely be the responsibility of the user,

and the user may be subjected to appropriate actions as decided by the authorities.

Policy violation

1. Violations any of this policy will be handled consistent with the institute disciplinary procedures applicable to the relevant users of the departments.
2. The institute may temporarily suspend, block or restrict access to information for _____days/month/year and network resources in order to protect the integrity, security, or functionality of institute's resources.
3. The College may routinely monitor network traffic to assure the continued integrity and security of College resources and maintain the record as documented proof against violation.
4. Confirmed violations will result in appropriate disciplinary action up to and including termination from employment or other relationships with the institute campus. In some circumstances, civil and criminal charges and penalties may apply.
5. Enquiries against the students will be enforced in case of any misbehavior or violation of the cyber security policy. All the staff members are empowered to initiate disciplinary action which in turn may lead to the constitution of an enquiry committee and further proceedings.

Investigation Functionaries Under the Code

Director
Deputy Director
Dean Academics
Heads of the Departments

Chief Rector of Hostel

Data-center In charge

Chair-person of ISC-Disciplinary Committee

Responsibility:

- As the persons in charge of the Departments/Hostels, the respective functionaries of all Departments and Hostels shall have the power and duty to take immediate action to curb any prohibitory behavior as envisaged under this code.
- The Director shall be the ultimate authority in imposing major sanctions as envisaged under any Section against the students for acts of prohibited behavior
- In the case of a confession by the student who violated the code of conduct, the sanctions shall be imposed or recommended.
- In the absence of confession, the complaint shall be properly enquired and the sanctions shall be imposed or recommended
- Director / Heads of Departments/ Chief Rector shall have the power and duty to call the Police immediately with the concurrence of the Director when there is a threat of Law and Order situation in the Campus
- The HoDs/ Chief Rector shall in such a case give a detailed report to the Director.
- The Director / HoDs/ Chief Rector can also arrange for video recording of the entire situation and take requisite actions through police and other concerned authorities
- For all disciplinary matters related to students, the Director shall be the ultimate authority as provided herein. Any person try to influence any of the authorities in implementation any of Policy, Student's Conduct and disciplinary code policy sections of the code shall be seriously viewed and action will be initiated against such person.

7.1 Mandatory disclosure with respect to I-CSC Usage Policy

To Whom this Document Concerns

All Users of IT infrastructure (Computers and the Network) at COEP.

Reason for Policy

This policy outlines the responsible use of the Information Technology Infrastructure at COEP

Statement of Policy

All users of COEP internet and computing devices will be subject to the following

Acceptable Use Policy.

1. [Content] I shall be responsible for all use of this network. In case I own a computer/computing device (notebooks, smart phones, tablets, iPhone, removable media) and decide to connect it to COEP network, I will be responsible for all the content on it, especially that which I make available to other users. In case I do not own a computer but provided some IT resources by COEP, I will be held responsible for the content stored in the designated workspace allotted to me (examples: file storage area, web pages, stored/archived emails, on Computer Centre or Department machines).

2. [Network] I shall be held responsible for all the network traffic generated by "my computer". I understand that network capacity is a limited, shared resource. I agree that physically tampering with network connections/equipments, sending disruptive signals, or making EXCESSIVE USE of network resources is strictly prohibited. Connecting of privately owned network devices such as (hubs, switches, repeaters, access points etc). to any of the network port of COEP is not permitted. Repeated offenses of this type could result in permanent disconnection of network

services. I shall not share the network connection beyond my own use and will not act as a forwarder/ masquerader for anyone else.

3. [Academic Use] I understand that the IT infrastructure at COEP is for academic/official use and I shall not use it for any commercial purpose or to host data services for other people or groups. Also, I shall not host or broadcast information that might harm others or may be otherwise considered objectionable or illegal as per Indian law.

4. [Identity] I shall not attempt to deceive others about my identity in electronic communications or network traffic. I will also not use COEP IT resources to threaten, intimidate, or harass others.

5. [Privacy] I will not intrude on privacy of anyone. In particular I will not try to access computers i.e hacking attacks , accounts, files, or information belonging to others without their knowledge and explicit consent.

6. [Monitoring] I understand that the IT resources provided to me are subject to monitoring, with cause, as determined through consultation with the COEP management, when applicable. The monitoring may include aggregate bandwidth usage to effectively manage limited IT resources as well as monitoring traffic content in response to a legal or law enforcement request to do so. I authorize COEP to perform network vulnerability and port scans on my systems, as needed, for protecting the overall integrity and efficiency of COEP network.

7. [Viruses] I shall maintain my computer on this network with current virus detection software and current updates of my operating system, and I shall attempt to keep my computer free from viruses, worms, trojans, and other similar programs.

8. [File Sharing] I shall not use the IT infrastructure to engage in any form of illegal file sharing (examples: copyrighted material, obscene material). In particular, I have noted the following:

Electronic resources such as e-journals, e-books, databases, etc. made available by the COEP Library are for academic use. These resources can be searched, browsed, and material may be downloaded and printed as single copies of articles as is done in the case of printed library material. Downloading or printing of a complete book or an entire issue or a volume of one or more journals (called systematic downloading) is strictly prohibited. Use of robots, spiders or intelligent agents to access, search and/or systematically download from the e-resources is also prohibited. Any violation of this policy will result in penal action as per the rules and regulations of the Institute. I am aware that Systematic downloading will result in the publisher blocking the entire community of users at COEP from accessing these resources.

9. [Security] I understand that I will not take any steps that endanger the security of the COEP network. Specifically, I will not attempt to bypass firewalls and access rules in place. This includes not setting up servers of any kind (examples: web, mail, proxy) that are visible to the world outside the COEP campus. In critical situations, COEP authorities reserve the right to disconnect any device or disable any account if it believed that either is involved in compromising the information security of COEP.

10. [Penalties] I understand that any use of IT infrastructure at COEP that constitutes a violation of COEP regulations or GOI regulation or is an offence under IT Act or other Acts framed by GOI from time to time, could result in administrative or disciplinary procedures apart from those admissible under relevant acts.

11. I will not hold COEP responsible for loss of any data or financial losses due to activities conducted over the COEP network. Since research materials in COEP are accessible to others, I promise to not transmit data that does not belong to me using the COEP network, failing which I will be penalized appropriately. I understand that access to the COEP network will be terminated when I cease to be part of the academic programs in COEP .

12. [Indemnity] I understand that COEP bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using these resources or facilities. I indemnify COEP against any and all damages, costs and expenses suffered by me arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by COEP.

Appendix (a)

Password reset form

To
The In-charge, Data-Center
COEP, Pune

Dear Sir/Madam,

I want to inform you that I have forgotten my password for COEP Moodle/ MIS/ Outlook and thus cannot access my COEP Moodle/ MIS/ Outlook account

I would, therefore, request you to regenerate/reset my Password for the said Account to assure an uninterrupted access in the future.

Sign :

Name :

Class & Branch :

MIS. No :

Mobile No :

E-Mail :

Date:

Recommended by Faculty Advisor

HOD

Data Center Use Only

Application Serial No. …….

Access granted on : …… by …… …

Data-Center In-charge
Sign

Appendix (b)

Wi-fi access application form

I ....., MIS No. ..... hereby declare that I am a student of COEP in the branch ... . I joined this college in the year..... I request you to kindly permit me to access Internet facility through Wireless connectivity provided at Data Center (DC) of the college.

The MAC address of the machine used by me for connecting to internet through this facility is ..... I assure to strictly follow the below mentioned conditions.

1. Connection will not be used for any illegal activities which may affect the goodwill of the college.

2. I will be the only person using the computer/laptop with this MAC address for wireless connectivity and will not transfer it to another person .

3. I agree to the condition that I will be the only responsible person for any activity happened through the IP address allotted to this MAC address which will come under the offence of Cyber law whichever is applicable.

Name : Student's Sign

Branch :

MIS. No :

Mobile and E-Mail:

Date:

Attached ID Proof as:

Recommended by Faculty Advisor

HOD

Data Center Use Only

Application Serial No. …….

IP No allotted to this MAC Address :

Access granted on : …… by ……

Data-Center In-charge Sign

Appendix (c)

Requisition form (For Faculty/Staff only)

Requisition form for Microsoft Outlook Email ID

Name: _____

Date of Joining (dd/mm/yyyy): _____

Department: _____

MIS No. : _____

Staff Name and Signature

Data Center Use Only

Application Serial No. …….

Access granted on : …… by …….

Data-Center In-charge Sign

Appendix (d)

Requisition form (For Students only)

Requisition form for Microsoft Outlook Email ID

Name: _____

Date of Admission (dd/mm/yyyy): _____

Tick Appropriate option

☐ BE First Year ☐ Direct Second Year

☐ M-Tech First Year ☐ Ph.D

Department: _____

MIS No. : _____

Student Name and Signature

Data Center Use Only

Application Serial No. …….

Access granted on : …… by ……

Data-Center In-charge Sign

Appendix (d)

Mandatory undertaking Form

I hereby declare that I have read the Cyber Security Policy Document of College of Engineering Pune (COEP) and understood all the terms and conditions of the same. I abide by the rules and regulations mentioned in the I-CSC Policy document.

Name: _____

Class/Designation: _____

Department: _____

MIS No. : _____

Date: _____ Signature: _____

Place: _____ Name: _____