Agnel Institute of Technology & Design

Assagao Bardez Goa

CSG/MIS Cell

AITD IT Infrastructure Usage Policy

Version 1.0

Date of Implementation	01st January 2018

A. Policy Statement

a. In its endeavor to provide all faculty, students and staff with a modern, fully networked computing and IT environment for academic use, the CSG Cell has decided to adopt the following AITD IT infrastructure usage Policy. The said policy will also be called the AITD IT Policy

b. Users of AITD computing, networking and IT facilities are expected to abide by the following rules, which are intended to preserve the utility and flexibility of the system, protect the privacy and work of students and faculty, and preserve our right to access the international educational networks to which the system is connected.

c. The AITD IT Policy applies to all staff, students of the institute and all other users authorized by the institute.

d. The AITD IT Policy relate to use of:

   i. All institute systems connected to the institute network.

   ii. All institute-owned/leased/rented and on-loan facilities.

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

   iv. To all institute-owned/licensed data/programs, on institute and on private systems

e. In case of any complaints personal/ departmental, appropriate action to be taken will be decided and taken by the person in-charge of the facility (the CSG Chair) in consultation with the Principal.

f. The objectives of the IT Policy and supporting policies are to

Principal
Agnel Institute of Technology and Design
Agnel Technical Education Complex
Assagao, Bardez - Goa

i. Ensure that information is created, used and maintained in a secured environment.

ii. Ensure that all of the institute computing facilities, programs, data, network and equipment are adequately protected against loss, misuse or abuse, viruses, worms etc .

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

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

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

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

B. <u>General IT Usage Policy</u>

a. Faculty, staff, and students may use the computing and IT facilities for academic purposes and official Institute business so long as such use

   i. does not violate any law, Institute policy or IT act of the Government of India.

   ii. does not interfere with the performance of Institute duties or work of an academic nature (as judged by CSG Chair and AITD Principal)

   iii. does not result in commercial gain or private profit other than that allowed by the Institute (through IRG).

b. Users are expected to respect the privacy of other users and they must not allow any other person to use their password or share their account. It is the users' responsibility to protect their account from unauthorized use by changing passwords periodically and using passwords that are not easily guessed. Sharing of passwords for any purpose whatsoever is strictly prohibited. The institute will not be responsible for any consequences that arise due to sharing of passwords. Users may share the required files through Google drive or other sharing software with proper access control.

c. Users should exercise care while entering their passwords at other non-trusted sites and should not be misled by purported emails from admin or other id.

d. Any attempt to circumvent system security, guess others' passwords, or in any way gain unauthorized access to local or network resources is forbidden.

e. Users may not use another person's computing account, attempt to forge an account identity, or use a false account or e-mail address.

f. Transferring copyrighted materials to or from the AITD systems without express consent of the owner is prohibited.

Principal
Agnel Institute of Technology and Design
Agnel Technical Education Complex
Assagao, Bardez - Goa

g. Downloading of copyrighted movies/books/games via torrent's or other means is traceable and staff and students are warned that on receipt of any complaints appropriate disciplinary action will be taken.

h. Downloading and installing of new software has to be done with the explicit consent of the respective facility in-charges in written and with prior permission from CSG Chair. Installation of unlicensed software on AITD facilities, or on individual machines connected to the AITD network, is strictly prohibited.

i. To the extent possible, users are expected to use only their official email addresses provided by AITD for official communications with other members of the Institute. Any complaints/requests to CSG must be made using your authorized email id otherwise we will not be able to verify your identity. In case for some reason you are not able to access your CSG email then you may write to us from your registered alternate mail id with us.

j. It is forbidden to use electronic mail and other network communications facilities to harass, offend, or annoy other users of the network, including impeding their computing systems, software, or data. It is also forbidden to send emails or messages masquerading as another person or to hide the sender's identity. Chain letters are not allowed. Neither is any form of commercial advertising, or soliciting allowed. Spamming is strictly disallowed. Subscribing to mailing lists outside the Institute is an individual's responsibility. Subscribing someone else to any group outside AITD is illegal.

k. It is forbidden to send frivolous or academically unimportant messages to any group. Broadcast of messages to everyone in the system is allowed only for academic purposes and emergencies. Violations of this (as decided by CSG Chair & Principal) will result in immediate freezing of the user's account for an extended period as determined by the CSG Chairs.

l. Shared email accounts for any purpose whatsoever are not allowed. All shared email accounts will be suspended with the notification of this policy.

m. Unauthorized use of institutional resources, including the transmission of pranks or false communications via email or messaging, is strictly prohibited and violators may face disciplinary action in accordance with the IT Usage Policy

n. Recreational downloads and peer to peer connections for recreational purposes are banned and are illegal.

o. To the extent possible, users are expected to connect only to the official AITD WiFi network for wireless access or any other WIFi network setup by the institute. Setting up of unsecured WiFI systems on the AITD network is prohibited.

p. Users are expected to take proper care of equipment, and are expected to report any malfunction to the staff on duty or to the in-charge of the facility. Users should not attempt to move, repair, reconfigure, modify, or attach external devices to the systems.

Principal
Agnel Institute of Technology and Design
Agnel Technical Education Complex
Assagao, Bardez - Goa

q. No food or drinks are permitted in the Computer Center or any labs. Smoking is strictly prohibited. Also making noise either through games/ music or even talking and/ or singing loudly is prohibited.

r. Playing of Games in Institute laboratories or using Institute facilities is strictly prohibited.

s. All cloud storage provisioned for the users will be used to store only institute related files.

t. Display or transmission of offensive material (either on computer screens, via emails, messages or through posters etc.) is strictly disallowed and serious action will be taken against offenders.).

u. IT Network Resource requirements for any workshops, conference should be communicated to the CSG Chair at least ten days ahead of the actual start of the event by the faculty in charge.

v. The IT infrastructure cannot be used to make any political statement or activity.

w. Sexual harassment of any type will not be tolerated in the computer lab. Transmission, viewing or accessing of any sexually explicit material is prohibited.

x. Student email accounts will remain active for a period of five years from the date of admission, after which they will be deactivated. Requests for extension of email accounts beyond five years will be considered on a case-by-case by the CSG Chair.

y. The maximum storage limit for student accounts on Google Workspace is 50 GB

C. **<u>Network access and monitoring policy</u>**

a. DHCP servers

i. The CSG Cell provides DHCP service to enable automatic IP configuration of personal devices clients. Installation of unauthorized DHCP servers, without explicit consent from the CSG, will not be permitted as such DHCP servers can interfere with normal usage.

ii. Use of static ip address without consent from the CSG Chair is strongly prohibited. Violation will result in immediate ban from AITD Network,

b. Wifi routers and access points

i. Installation of unprotected WiFi routers is prohibited.

ii. Installation of Wifi routers in the academic area will not be permitted without explicit consent from CSG.

iii. All users should use the authorized AITD_WIFI SSIDs for WiFi access and verify the authenticity

iv. Access to AITD WiFi is restricted & only users permitted by CSG will be allowed access to AITD WiFi.

v. Students Mobile devices are disallowed on AITD WiFi.

1. Any request for allowing student mobile devices on AITD WiFi will be purely for academic purposes

Principal
Agnel Institute of Technology and Design
Agnel Technical Education Complex
Assagao, Bardez - Goa

        2. Access permission will be granted only after a written request from the concerned faculty & approved by the HoD the student belongs to.

c. Connecting other ISP networks to AITD LAN
    i. It is strictly prohibited to connect other ISP networks (not obtained through CSG) to the AITD LAN without explicit consent from CSG Cell. In case it is allowed due to research or operational needs it will be the responsibility of the facility in-charge to completely firewall the external network from the AITD LAN, both for inward and outward connections.

d. VPN and ssh access to AITD LAN
    i. It is strictly prohibited to setup unauthorized VPN or ssh access facilities for connecting to AITD LAN from outside without explicit consent from CSG.
    ii. It is also prohibited to facilitate external access to the AITD network using any terminal sharing, file sharing or other similar software.

e. Access monitoring in AITD VLANs
    i. ARP monitoring is to be enabled on all LANs and all IP address to MAC address mappings will be logged and maintained for a period of three months.

f. Internet access (wireless LAN)
    i. Connecting to the SSIDs AITD_WIFI, AITD_GUEST will require 802.1x authentication and all wireless network traffic will be encrypted using WPA/WPA2 standards.
    ii. All authentications will be logged along with time of access, uid of the user, registered DHCP IP address and the MAC address of the accessing device.
    iii. All authentications will be MAC based for AID_WIFI SSIDs

g. Static IP addresses for inward connections
    i. On special requests static external IP addresses may be allocated to specific servers for access from outside on specific ports. This may be required for designated web servers and other research facilities.
    ii. In all such cases it will be the responsibility of the faculty in-charge to install proper firewall and security measures to ensure that the access is restricted to the specific server and the AITD network is completely protected from external accesses.
    iii. No shell or VPN access should be provided without explicit consent of CSG.

h. Unrestricted external access from designated servers
    i. Unrestricted access to internet access bypassing the firewall may be given from specific machines on request for special research and operational

Principal
Agnel Institute of Technology and Design
Agnel Technical Education Complex
Assagao, Bardez - Goa

needs. It will be the responsibility of the faculty in-charges to ensure that the resources are used for the intended purpose only.

ii. For unauthorized access the staff Chair needs to send a written request to the CSG Chair & Principal approved by the HoD of the respective department.

D. Violation of Policy & Reporting of Security Incidents

a. Violations of policy will be treated as academic misconduct, misdemeanor, or indiscipline as appropriate. Depending upon the nature of the violation, CSG Chair may take an action by issuing a warning through disabling the account and for routine infractions, appropriates fines/penalties as determined by the Institute

b. In case of repeat offenders or other extreme cases the user may be prohibited access to IT facilities at AITD permanently, and/ or other appropriate action as determined by Institute authorities.

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

d. Incidents can be reported via:
   i. Email (csg@aitdgoa.edu.in)
   ii. Appointment with CSG Chair (Any time)

e. In the event of a suspected or actual breach of policy,
   i. The CSG Chair will report to Principal
   ii. Unsafe users institute accounts would be disabled & access bared
   iii. Appropriate fines will be charged by the CSG Chair for the replacement cost of the stolen/damaged asses.
   iv. Institute will go ahead with Legal implication if necessary

f. The CSG Chair can disable access to any IT infrastructure of the institute for any user without prior intimation.

E. IT Infrastructure Monitoring & Audit

a. The CSG cell will monitor network activity, reports from the service providers and take action/make recommendations consistent with maintaining the security of institute information systems.

b. CSG Cell will regularly monitor network access & access to IT Infrastructure.

c. The

d. All IT infrastructure of the institute will be audited by the CSG Chair or teams appointed every six months.

e. The CSG Chair can initiate the audit of any IT infrastructure or systems of the institute at any time if required.

F. Compliance with Legislation

Agnel Instit..
Agnel Techn..
Assagao, -

a. The institute, at its discretion, may also disclose the results of such monitoring, including the contents and records of individual communications, to appropriate institute authorities or law enforcement agencies under applicable laws, and may use those results in appropriate disciplinary proceedings

G. Changes to Policy

a. The policy may change as and when it is considered appropriate and new policies or the changes in policy will take effect immediately after a brief announcement by any means, e-mail, printed notices, or through groups.

Principal
Agnel Institute of Technology and Design
Agnel Technical Education Complex
Assagao, Bardez - Goa