10, Institutional Area, Vasant Kunj,
New Delhi 110 070

MINUTES OF THE THIRTY NINTH MEETING OF THE BOARD OF MANAGEMENT

The Thirty-ninth meeting of the Board of Management was held on 14th August, 2021 at 10:30 hours online on Microsoft team platform. The following were present:-

PRESENT:

Members
Professor Eklabya Sharma, Chairperson
Professor Manipadma Datta
Dr V P Singh
Dr Nimmi Singh
Dr Sachin Chaturvedi
Professor George John
Dr Bhim Singh
Professor Arun Kansal
Professor Shaleen Singhal
Professor Ramakrishnan Sitaraman
Mr Kamal Sharma, Secretary

Special Invitees
Dr Vibha Dhawan
Dr Manish Shrivastava
Dr Fawzia Tarannum
Mr Dhanraj Singh
Ms. Pooja Chaudhary

Leave of absence: Professor E Somanathan and Mr RR Rashmi could not join the meeting.

Item No. 1: To confirm the minutes of the Thirty Eighth meeting of the Board of Management held on 29 December 2020.

It was informed that the minutes of the Thirty Eighth meeting of the Board of Management held on 29th December, 2020 were circulated to the members of the Board and no comments had been received on the same.

TS/BM/39.1.1. The Board resolved that the minutes of the 38th meeting of the Board of Management held on 29th December, 2020 be confirmed.

Item No. 2: To consider and approve Policy on Research Promotion

The Registrar requested Prof. Shaleen Singhal, Dean (Research & Relationships) to present the policy.

Prof. Shaleen Singhal informed that the Vice Chancellor has set up a Committee to look into the institution research facilities and come up with a policy for promotion of research at the TERI SAS and an Action Plan for its adoption and

implementation. The Committee has prepared a draft policy on Research Promotion and is presented to the Board as placed in **Enclosure 1**.

Prof. Sachin Chaturvedi lauded the efforts put in preparing the Policy on Research Promotion and said that the Institution Innovation Council and Entrepreneurship Development Cell of the institution should work together. Research accomplishments of students should be highlighted and it would be good to engage the students in more research activities. It would be good to showcase the achievement of the students. Dr Nimmi Singh suggested that it would be good to collaborate with companies from the beginning which would be helpful in filling up the data gaps. Prof. Bhim Singh said it would be a good initiative to set up a separate cell which could collaborate with government agencies for funding. Prof Ramakrishnan suggested allocation of bridge funding in the research policy and a provision for incentive be included in the policy. Prof. Eklabya Sharma welcomed the suggestions of the members and said that showcasing student research activities is important which can enhance TERI SAS' reputation. He requested that the suggestions of the members to be incorporated in the policy.

TS/BM/39.2.1 The Board resolved to approve the Policy on Research Promotion after incorporating the suggestion of the members as placed in **Enclosure 1**.

Item No. 3: To consider and approve the amended rules for the Students Council

The Registrar requested Dr Manish Shrivastava to present the matter to the Board. Dr Manish Shrivastava informed that the rules for the Students Council at TERI School of Advanced Studies were approved in the 35th BoM meeting held on 29th July, 2020 (TS/BM/35.5.1). Based on the comments received during the operationalising of the rules, a Committee was set up to review the rules and the revised rules are presented to the Board as placed in **Enclosure 2**.

TS/BM/39.3.1 The Board resolved to approve the amended rules for the Students Council as placed in **Enclosure 2**.

Item No. 4: To consider and approve IT Policy of TERI SAS

The Registrar requested Dr Fawzia Tarannum to present the IT Policy of TERI SAS. Dr Fawzia Tarannum explained in detail to the Board members the IT Policy of TERI SAS as placed in **Enclosure 3**. With regard to the validity of the students' official email ID for life time, Board members raised their apprehension and suggested suitable security measures should be taken so that it cannot be misused. Members suggested that strong cyber security and monitoring mechanism should be in place and provision of deactivation should be there. Proper handing over and taking over should be in place. Prof. Eklabya Sharma welcomed the views of the members and informed that the suggestions would be incorporated in the revised policy and be sent to the Board members for approval along with the minutes.

TS/BM/39.4.1 The Board resolved to approve the IT Policy of TERI SAS after taking into consideration the suggestions put forth by the members and as placed in **Enclosure 3**.

Item No. 5: To consider and approve the formation of the Institutional Ethics Committee

The Registrar requested Prof. Shaleen Singhal to inform the Board Members about the matter.

Prof. Shaleen Singhal informed that the Institutional Ethics Committee was constituted on 7th July, 2021 vide Notification No.46 of 2020-21 to address ethical issues relating to research and consultancy engagements as placed in **Enclosure 4**. He further stated that detailed note along with Terms of Reference of the Committee will be formulated and approval of the Board members will be sought but in the meantime he requested the Board members to approve the formation of the Institutional Ethics Committee.

TS/BM/39.5.1 The Board resolved to approve the formation of the Institutional Ethics Committee as placed in **Enclosure 4**.

Item No.6: To record approval by circulation of BoM for opening FCRA account: Presently, TERI SAS is having its FCRA bank account with HDFC Bank Limited, Surya Kiran Building, New Delhi - 110001. As per the Foreign Contribution (Regulation) Amendment Act, 2020, the FCRA registered associations have to open a mandatory FCRA bank account only with the State Bank of India, New Delhi Main Branch, 11, Sansad Marg, New Delhi - 110001. Hence approval by circulation was sought from Board members on 21 June 2021 on the resolution to be submitted to the State Bank of India for opening of the FCRA Account. On receipt of signed documents from the Board members, it was submitted to the State Bank of India and FCRA account has been opened. Dr Ramakrishnan suggested that the Vice Chancellor's name should be there as one of the signing authorities for operation of the FCRA account. Prof. Eklabya Sharma informed that since he was not in station at the time of opening the account and hence the account was opened without including his name but now since he has joined back, his name be included for operation and maintenance of the FCRA account.

The Board noted the matter.

Item No 7: To consider and approve audited statement of accounts of the financial year 2019-20

Mr Dhanraj Singh, Project Management and Deputy Finance Officer, informed that the audited accounts for the financial year 2019-20 are attached as **Enclosure 5**. The Board is requested to approve the financial accounts for the period 2019-20.

Enclosure 3

IT Policy

LAN & Desktop connection policy

For Faculty members and Administrative Staff

- The request to generate username and password for login into the domain system () is made from the registrar office.
- The convention used for creating the user id is FirstName.LastName@terisas.ac.in For e.g. A person with first name as Ajay and last name as Sharma shall be assigned the user id as ajay.sharma@terisas.ac.in . The assigned password can be changed after logging in for the first time.
- After Login, the following network/share drive are accessible by default
    a. A common scratch drive (S :\) for data sharing within TERI SAS. The files will remain there for 24 Hours only. It can also be deleted earlier in case the need arises.
- Software Restrictions is enabled: Users are not allowed to install any software on his/her desktop computing system. However, they can reach out to the administrator in case they have a requirement to install software on their system.
- Default TERI SAS wallpaper is enabled, and the user does not have the rights to change it.
- Basic softwares like MS Office 2010/2013/2016, Adobe Reader, Chrome and IE9 etc. are preinstalled in the system.
- The system has a Screen Saver Policy which allows it to hibernate after 45 minutes of idle state. The screen locks after 15 minutes of idle time.
- Specialized hardware and software are provided after approval from the competent authority.

For students

- Students are assigned a username and password at the time of joining. The convention that is followed is like the admin and faculty members. In case there are two or more students with similar names a numeric digit starting from 1 is added after the last name. E.g Another student by the name Ajay Sharma shall be give the mail id as ajay.sharma1@terisas.ac.in.
- Common username and password are used by the students to login and access the LAN system. Default TERI University wallpaper is enabled at the time of access which cannot be changed.
- Basic softwares like MS Office 2010/2013/2016, Adobe Reader, Chrome and IE9 etc. are preinstalled in the system.
- The system has a Screen Saver Policy which allows it to hibernate after 45 minutes of idle state. The screen locks after 15 minutes of idle time.
- After Login, the following network/share drives are accessible by default.
    a. A common scratch drive (S:\) for data sharing within TERI SAS. The files will remain there for 24 Hours only. It can also be deleted earlier in case there is a low space warning.

- Specialized software is installed on the lab systems, like ArcGIS, ERDAS in the GIS Lab, MATLAB, RET Screen, Homer, Stata, etc. in computer Lab. Student can access these systems and use them during the allocated time or with prior permission of the Lab In-charge

Backup Policy

- Dedicated backup system is implemented for backup and recovery of data stored in the Active Directory files system.
- Full back up of DC (Domain Controller) machine data is taken monthly and is stored in the tape drives and stored in a safe place.
- Auto-Backup of portal server's database is taken on daily basis and the codes are backed up on monthly basis in OneDrive then later its stored in the tape drive and kept in a safe place.
- Backup of individual users is taken only when a request is made to the IT Help desk, otherwise all the users are instructed to copy their data in their OneDrive. Restoration is done as per the need and request by the user. Backup of critical users is taken in external Hard Drive which is then copied to a tape and as per the request of the user it is extracted and given back to them.
- To ensure that all data related to the departments are retrievable, a folder for each department shall be created in the shared drive of the University. Faculty members and Program Assistants shall save everything related to the administration, projects, and activities of the department on the shared drive in the assigned folder. The edit and delete rights of the files once placed in the shared drive shall be with the system administrator only.

Wi-Fi Policy:

- The Wireless network for Internet access for the Students, Hostellers, Staff and Guests is separate from the office LAN.
- Wi-Fi Access points are available on the Academic, Dining, Admin blocks and in the hostel. There are some areas on campus where the signal strength may not be very good.
- WPA2-Enterprise encryption and network user id and password is required for connecting to the WiFi.
- User id & Password to connect to the WiFI is shared with every faculty, student and staff by the IT Helpdesk
- Guests can take coupon from the reception to access the WiFi. However, such coupons are issued only after verification of the guests' identity.
- Full bandwidth is allocated to Students and Hostellers after office hours that is from 5.30 PM till 7AM.

Printing policy

- Printers are installed in the identified location for the staff and faculty members only.
- All printers are with credential security system and require password to enable printing.
- Network Multi-Functional devices with both black and white and colour printing facility and features to print, scan and photocopy are installed in the administrative department.
- For students, third party printing facility is available in the basement.
- The configuration of the printers are as follows:
    a. Two Printers are Capable of printing A3/A4 sizes.
    b. Duplex printing with auto feeder.
    c. Canon printers can Scan and send to a file (shared folder).
    d. All printers have photocopy feature.

Network

- Connectivity from TERI SAS to TERI-IHC is with NDE leased circuits.
  I. **2** NDE Links: From TATA Communications
  II. ILL Link: From TATA Communications
- Capacity:

I.	ILL:	**100** MBPS	
II.	NDE Link:	**18** MBPS	TERI SAS – TERI IHC
III.	NDE Link:	**18** MBPS	TERI SAS – DATA CENTER

- Floor-wise VLAN is created to create smaller broadcast domain.
- The switches are configured with Storm-Control feature to disable the port in case the broadcast OR multicast traffic reaches the threshold limit of 1 mbps
- There are few ports in the selected location where no storm-control feature is enabled for WebEx and Printers.

EMAIL POLICY

TERI SAS

10, Institutional Area,

Vasant Kunj.

Email Policy

Purpose

The purpose of this policy is to describe the acceptable use of Email service to support, research and administrative functions. The institute encourages the use of email system to share information, to improve communication, to exchange ideas and to transact business.

It is aimed to ensure that email service remains available and reliable and is used for purposes appropriate to the mission of the institute. Users have the responsibility to use this resource in an efficient, effective, ethical, and lawful manner.

Scope

This policy covers appropriate use of any email sent from a TERI SAS email address and applies to all members (Faculty, Staff and Students) of the institute who are entitled to email services for sending and receiving email messages and attachments.

Email usage

General use

TERI SAS main purpose of providing email services is to share information, to improve communication, to exchange ideas and to impart education. This facility should not be abused by any user of the institute which includes but not limited to:

- Creation and distribution of content which brings dishonor to the institute
- Creation and distribution of illegal content
- Distribution of unsolicited commercial or advertising material and other junk email of any kind
- Unauthorized transmission of any confidential content of the institute
- Transmission of content which is the copyright/ intellectual property rights of another person/ organization
- Activities that unreasonably waste staff effort or IT resources, or activities that unreasonably serve to deny service to other users

- Activities that corrupt or destroy other user's data or disrupt the work of other users
- Unreasonable or excessive personal use
- Creation or transmission of any offensive, obscene, or indecent images, data or other material
- Creation or transmission of material which is designed or likely to cause annoyance, inconvenience, or anxiety
- Creation or transmission of material that is abusive or threatening to others, serves to harass or bully others, discriminates, or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs
- Creation or transmission of defamatory material or material that includes claims of a deceptive nature
- Activities that violate the privacy of others or unfairly criticize, misrepresent others; this includes copying distribution to other individuals
- Creation or transmission of anonymous messages or deliberately forging messages or email header information, (i.e., without clear identification of the sender) or for 'flaming'
- The unauthorized provision of access to University services and facilities by third parties

Personal use

The institute allows reasonable level of email services for personal use. An absolute definition of abuse is difficult to achieve but certainly includes (but is not necessarily limited to):

- A level of use that is not detrimental to the main purpose for which the facilities are provided
- Priority must be given to use of resources for the main purpose for which they are provided
- Not being of a commercial or profit-making nature, or for any other form of personal financial gain
- Not be of a nature that competes with the Institute in business
- Not relate to any use or application that conflicts with an employee's obligations to the institute as their employer

- Not be against the Institute's rules, regulations, policies, and procedures and in particular this email policy

Microsoft Outlook

- The Office 365 license for Educational Institutes is free
- MS Office applications i.e., MS Word, Excel & PowerPoint are essentially required applications for education and research work. But the desktop version of MS Office is not free for educational institutes like TERI SAS and many others.
- All students get web version of MS Office applications free in addition to all other Office 365 applications.
- The Office 365 platform have following useful applications required for TERI SAS Operation:
  - **a.** Outlook: 50 GB mailbox
  - **b.** TEAMS
  - **c.** ONE DRIVE: 1TB space on cloud mapped with local system
  - **d.** SHAREPOINT
  - **e.** MS PLANNER
  - **f.** STREAM VIDEO
  - **g.** One user license of Office 365 valid on 5 devices
  - **h.** Students get online version of word

Single Sign-on: all applications of Office 365 are integrated and only one login required

Usage monitoring

TERI SAS accepts that the use of email is a valuable productivity tool. However, misuse of this facility can have a negative impact upon productivity and the reputation of the institute.

In addition, all the institute's email resources are provided for official work purposes. Therefore, the institute maintains the right to examine any systems and inspect any data recorded in those systems.

To ensure compliance with this policy, the institute also reserves the right to use monitoring software in order to check upon the use and content of emails. Such monitoring is for legitimate purposes only and will be undertaken in accordance with a procedure agreed with the employees. Therefore, employees shall have no expectation of privacy in anything they store, send, or receive on the institute's email system.

General Guidelines

Quotas and limits

All users have access to the centrally managed email server. All accounts have quota limits placed on them as listed below:

Default mailbox Size of all users is 50 GB and attachment (sending & receiving) size is limited to 35 MB.

Users shall receive email notification when they are approaching their quota limit and are encouraged to follow guidance in the email to manage their account. The mails will be delivered to the inbox only till such time that the quota is available. Once filled, the delivery of the emails shall be suspended till the time the inbox is cleared to create the storage space.

There are limits on the size of an email that can be received and transmitted. No email greater than 35 MB can be accepted for transmission by the email servers.

Mailing Groups

A new user is added to different mailing lists as per his/ her role in the organization at the time of account creation. The different mailing groups are described below:

- **Administrative staff:** admin-tu
- **Faculty staff:** Faculty
- **Student:** Students
- **Program:** Programme short name followed by year.
- **Personal group:** Users can create their own personal mailing list for specific activity requirement

Calendar / Scheduling

The Calendar option is provided in the Outlook where the user can view their calendar entries like meetings, appointments etc. for a day, week or month by selecting the different viewing options. The user can also view the availability of other colleagues and from there one can schedule the meeting/ appointment.

Access Modes

The emailing and collaboration applications can be accessed through the following three modes:

a) Desktop Application

The desktop application which is by default installed at the time when a system is allocated to a user to access the emailing and collaboration services.

b) Outlook Web App (OWA)

The user can also use the applications to access the emailing functionality along with other Office 365 products through any web browser connected to the internet by browsing the URL: portal.office.com

c) Mobile App

The applications can also be accessed through mobile apps. For e.g. users can download the app "**Microsoft Outlook"** from the App Store to access the emailing functionality. The app provides all the notifications related to emails and reminders to the user.

Virus checking

Computer viruses, trojan horses and worms are collectively known as malware. One common method of distributing malware is via email. All email communication through the Computer Services email gateways is checked for malware. Checking strategies include refusing messages containing executable attachments, scanning messages for known malware or a combination of both techniques. Please note that this is a separate procedure and not related to the virus scanning policy applied to the central fileserver.

The sender of messages containing malware will be informed of the viral content of their email. A similar message will be sent to the administrator of the email server.

Email Security

Email provides an important platform for cyber-attacks. Phishing is one such important form of attacks. It refers to emails that appear to be coming from a legitimate source but are infact scams that are designed to steal sensitive private information.

Thus employees are requested to follow the below instructions:

• Be suspicious of unknown links or requests sent through email or text message.
• Do not open email attachments from unknown sources, and only open attachments from known sources after confirming the sender.
• Click on links in emails cautiously.
• Do not respond to requests for personal or sensitive information via email, even if the request appears to be from a trusted source.
• Verify the authenticity of requests from companies or individuals by contacting them directly.
• Sending of any proprietary information via email should be done cautiously and sharing of sensitive information like credit card details should be avoided.

Usage Monitoring

The institute's email services are provided for official work purposes. To ensure compliance with this policy, the institute reserves the right to monitor the use and content of the emails.

Such monitoring is for legitimate purposes only and the employees shall have no expectation of privacy in anything they store, send or receive on the institute's email system.

Aliases and lists

All members of staff will be allocated email aliases based on their First name and Last name. Email alias duplications are possible, so it is sometimes not possible to offer the exact email alias to users. Specific email aliases can be requested for individual or group use if there is a legitimate requirement. Email aliases will not be changed for arbitrary or trivial reasons and the final decision on whether a reason is valid lies with IT Services.

Email distribution lists are created for various institutional groups like Administrative, Faculties, Students, Programme, location-based etc. Generally, individuals requesting a list will be responsible for the ownership and management of the list.

Automatic email forwarding

Automatic forwarding or redirection of email to other mail domains is possible. IT Services is not responsible to forward emails outside the TERI SAS network. It is the individual's responsibility to set forwarding rule and make sure the forwarding address is correct and the email service being used is reputable and reliable. Users must exercise caution when automatically forwarding any email to an outside network and question the need to even do so. All our email services are accessible to authorized users from the Internet.

Automatic forwarding or redirection of email within the terisas.ac.in mail domain is not allowed. Allowing other people to access email can be achieved directly by delegation of mailbox.

Logging

Traffic through the IT Services email gateways is logged. Logs include details of the flow of email but not the email content. Transaction logs are kept online for 30 days. Logs are available to authorized systems personnel for diagnostic and accounting reasons.

Standards

Standards are adhered to wherever possible. The IT Services email gateways will attempt to verify the source and destination of email before being passed on. The postmaster and abuse email addresses are implemented in accordance with RFC 2142.

Spam and junk mail

Spam can be defined as "the mass electronic distribution of unsolicited email to individual email accounts". Junk mail is usually a result of spamming. In reality spam and junk mail are regarded as interlinked problems.

A certain amount of junk mail is blocked at the mail gateways. Any mail reaching the email gateways which has been marked by these services will be rejected. Incoming email is also checked against for Spam and junk by a third part anti-spam service.

Incident handling and data protection

The institute will investigate complaints received from both internal and external sources, about any unacceptable use of email that involves IT Services. IT Services, in conjunction with other departments as appropriate, will be responsible for the collation of information from a technical perspective. It should be noted that logs are only kept for limited periods of time so the prompt reporting of any incidents which require investigation is recommended.

Where there is evidence of an offence it will be investigated in accordance with the institute's disciplinary procedures applicable to all members of the institute. In such cases IT Services will act immediately with the priority of preventing any possible continuation of the incident. That is, accounts may be closed or email may be blocked to prevent further damage or similar occurring.

Password Protection

Institute’s policy requires the use of strong passwords for the protection of email. A strong password should contain digits, special characters as well as letters. The IT Passwords Policy contains information on how to choose and maintain compliant passwords.

Mass mailing

Institute may use email to market to existing and potential customers. There is significant legislation covering bulk email and use of email for marketing through CRM account. Users must not send bulk emails using the standard email system by doing so their email account will be blocked by default email policy.

Email Account Management

7.1 Individual user account

Email id length:

- FIRST NAME (.) LAST NAME @ TERISAS.AC.IN **(PREFERRED)**
- FIRST NAME (.) FIRST INITIAL OF LAST NAME @ TERISAS.AC.IN (IN CASE OF LONG NAME)

- FIRST NAME (.) LAST NAME FOLLOWED BY NUMBERS (2), (3) @ TERISAS.AC.IN (IN CASE OF SAME NAME EXISTS)

1.2 Account deactivation

Staff/Faculty Email id: Following action is taken when any staff member gets a Clearance Form signed by the IT Department at the time of leaving the institute.

- Account is deactivated after one month of leaving the institution.
- Membership of any distribution list is revoked.

If the user requires their account to remain active for a certain period, she/he must get a written approval from appropriate authority namely VC / Registrar / HoDs.

The HoD/Registrar shall ensure that there is a proper handing over of all data relevant to the projects/portfolio being handled by the outgoing staff/faculty.

Student Email id: Students are permitted to retain their university e-mail id till one month after the convocation. The institute mail id is deactivated thereafter. The personal e-mail ids of the graduating students are collected at the time of submission of the clearance form. Every graduating student's mail id gets added to the group id alumni@teriuniversity.ac.in which is used for all future communications with the Alumni.

In case any alumnus approaches the university to access the university id mailbox, he/she is provided temporary access after approval of the request from the Registrar. Graduating students are encouraged to use the message forwarding feature in Office 365 to divert their mails to their personal ids.

1.3 Proxy Access

An approval-based provision for Proxy Access has been provided through which an employee can provide proxy access of his/her mailbox to some other colleague for e.g. the Directors can delegate their mailbox access to their Secretary.

Benefits for Students

It may be noted that academic institutes that are Microsoft customers and hold licensed Office Software at the institutional level are eligible to offer Office 365 to their students at no extra cost.

Also, students can take benefit of free Office 365 by logging in to the Office 365 portal. The services which are included in it are Office Online (Word, PowerPoint, Excel, and OneNote), 1TB of OneDrive storage, Microsoft Teams, Yammer, and SharePoint sites.

Since Office 365 is based in the cloud, it can be accessed for anywhere and from any device like mobiles, tablets, and laptops on the go. It can help to maintain record of all communications, documents, meetings, and other items without any additional cost.

It allows better collaboration as it permits team members to edit one document. Microsoft Office 365 offers increased storage, accessibility, and file sharing from wherever you may be as well as 1TB Mailbox.

Service Level management

Monitoring and Performance of the Email System

Managed by Microsoft Office 365 Cloud solutions

Review

This policy will be reviewed annually or as and when required at any point of time during the year.