SUKKUR IBA UNIVERSITY

MERIT - QUALITY - EXCELLENCE

No: SUK-IBA/Rgr/251/24

Date 02 - 02 - 2024

NOTIFICATION

Consequent upon the approval of the Syndicate vide resolution# 18.69 in the 18th Meeting of Syndicate, Sukkur IBA University held on December 08-09 & 16, 2023, the Vice Chancellor, Sukkur IBA University has been pleased to approve the ICT Policy of Sukkur IBA University.

The copy of ICT Policy of Sukkur IBA University is attached **Annexure – A**

Azhar Ali Soomro
Registrar
Sukkur IBA University

Cc to:

1. ES to Vice Chancellor
2. PVC
3. All Deans/HoDs/Sectional Heads
4. All Directors
5. Internal Auditor
6. Director Finance
7. All Concerned

Sukkur IBA University

ICT Policy

Submitted by:

Committee Members

(Office Order, NO: SUK - IBA / Rgr / 332 / 23 Dated 04-03-2023)

TABLE OF CONTENTS

IT Policy of Sukkur IBA University

In pursuance of Office Order, NO: SUK - IBA / Rgr / 332 / 23 Dated 04-03-2023 and Consequent upon the approval of the Vice Chancellor, Sukkur IBA University the Committee has been constituted to draft the IT Policy of Sukkur IBA University.

ToR of the Committee:

1. To draft IT Policy for Sukkur IBA University and the recommended steps for establishing and implementing a modern IT infrastructure.

2. To draft IT internal control framework, advice on Gmail Storage Policy and consider suitable strategies, structures, and sizes for the emailing function.

3. To review Internet social media Policy, whereas students' access to the social media app will be restricted during academic hours and use social media apps appropriately and responsibly and should not engage in any behavior that may damage the reputation of the university.

4. To review Internet quality of service and its efficient usage in campus. In this regard, committee recommended to limit the number of devices i.e. Faculty and staff can use five devices and students can use only two devices.

SIBAU and HEC PERN Agreement

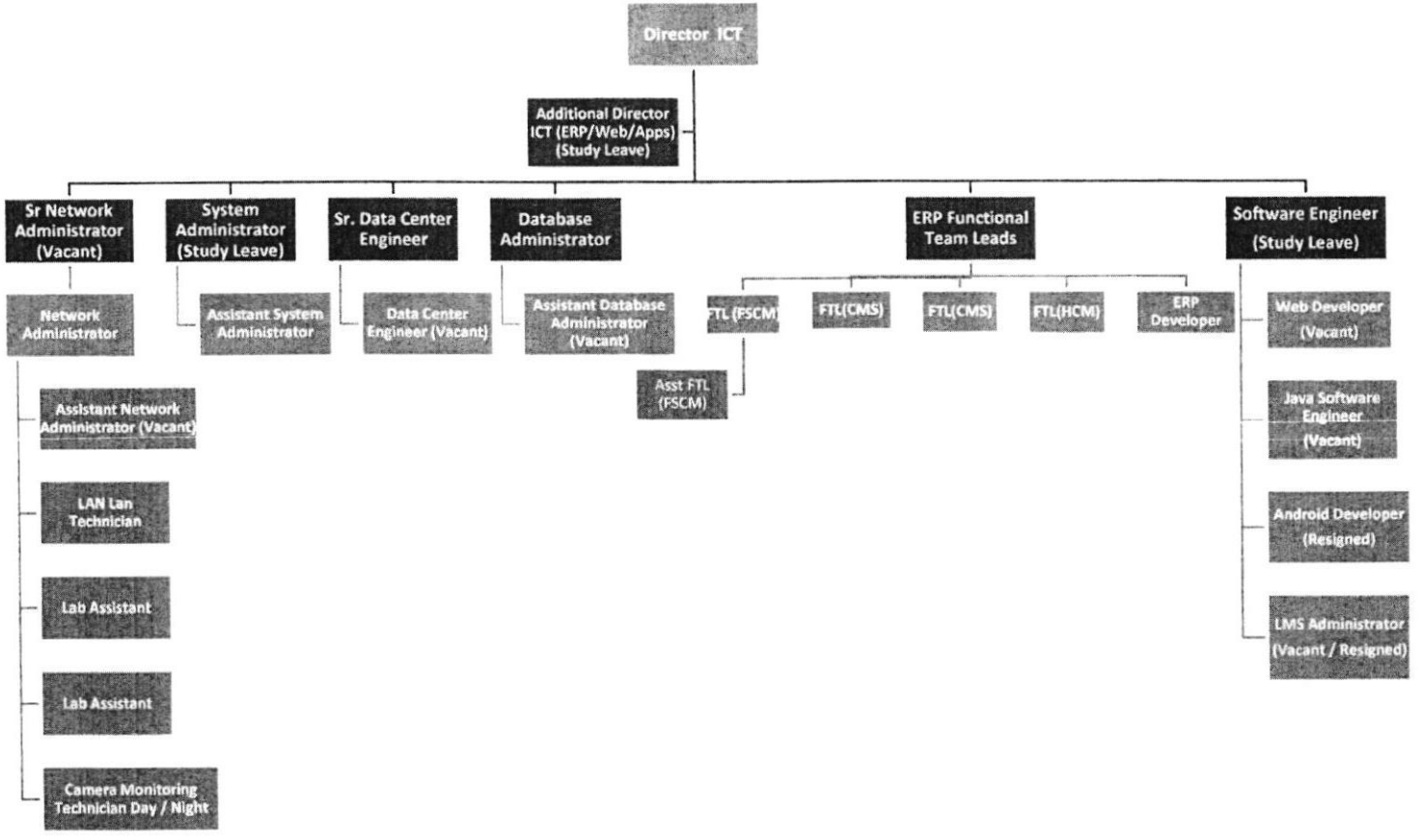
Sukkur IBA University (SIBAU) is a renowned public university located in Sukkur, Pakistan. It offers a diverse range of undergraduate and graduate programs in various disciplines. As an esteemed member of Pakistan's education and research community, SIBAU has established a valuable partnership with the Higher Education Commission (HEC) to connect to the Pakistan Education and Research Network (PERN).

Through this collaboration with HEC, SIBAU gains access to high-speed internet connectivity and a wide array of academic resources and services available via PERN. PERN, dedicated to serving educational and research institutions in Pakistan, facilitates internet connectivity and related services essential for academic excellence.

By leveraging its connection to PERN, SIBAU can tap into an extensive collection of academic resources and tools, including e-journals, research databases, and specialized software, greatly enriching its teaching and research endeavors. Additionally, PERN offers an array of supplementary services such as video conferencing, web hosting, email, and cloud services, empowering SIBAU to enhance its teaching methodologies and research capabilities.

The agreement with HEC ensures that SIBAU can fully benefit from PERN's robust network infrastructure and services, which are crucial for delivering quality education and conducting impactful research. By being a part of PERN, SIBAU fosters collaborations with other esteemed educational and research institutions across Pakistan and globally, fostering a vibrant academic environment and further elevating its teaching and research initiatives.

PROPOSED ORGANOGRAM OF ICT DEPARTMENT



LMS (E-Learning for Faculty and Students)

1. Introduction

This policy outlines the guidelines and procedures for the effective use of Information and Communication Technology (ICT) in e-learning initiatives for faculty and students. The purpose of this policy is to ensure the successful implementation of e-learning programs, promote digital literacy, and provide faculty and students with the necessary resources and support to engage in meaningful online learning experiences.

2. Scope

This policy applies to all faculty members and students participating in e-learning activities that involve the use of ICT within the organization.

3. Infrastructure and Technology

3.1.1. Reliable Internet Access: Faculty members and students should have access to a reliable internet connection to engage in e-learning activities without interruptions.

3.2. Hardware and Software Requirements: Faculty members and students should have access to the necessary hardware (e.g., computers, laptops, tablets) and software applications (e.g., learning management systems, collaboration tools) required for effective participation in e-learning activities.

3.2. Technical Support: Sufficient technical support services must be accessible to provide assistance to faculty members and students in resolving any ICT-related issues that may arise during e-learning activities. For comprehensive guidelines and instructions, kindly refer to the official website, YouTube channel, and the provided links.

http://elearning.iba-suk.edu.pk/

https://youtu.be/gVQhI8TPcjI?list=PLZEUzxOCM8bvLfU_bSC72eCO2loTXPSpJ

https://drive.google.com/file/d/199yRnPllGabJ-Ax4LHnbf3J__QxB0hrS/view

https://drive.google.com/file/d/1b9X4NmkEOTug8T2_4HdYzrLBhkUOqF91/view

4. Faculty Responsibilities

4.1. Technological Proficiency: Faculty members should possess the necessary technological skills to effectively use ICT tools, platforms, and resources in the e-learning environment.

4.2. Course Design and Delivery: Faculty members are responsible for designing and delivering online courses that leverage appropriate ICT tools, ensuring they align with the organization's learning objectives and standards.

4.2. Course Storage and Retention: Faculty members are encouraged to utilize cloud storage options such as Google Drive, Microsoft OneDrive, and YouTube to upload recorded videos and share the corresponding links on the Learning Management System (LMS). The ICT Team will be responsible for retaining the courses of the last two semesters on the LMS server. Faculty members are advised to keep backup copies of their courses on their local storage as well as cloud storage for additional redundancy and security.

4.3. Communication and Collaboration: Faculty members should establish clear channels of communication and facilitate effective collaboration among students using ICT tools and platforms.

4.4. Assessment and Feedback: Faculty members should utilize appropriate ICT tools and platforms for online assessments, providing timely feedback to students on their performance and progress.

5. Student Responsibilities

5.1. Technological Readiness: Students should possess the necessary technology skills and ensure they have access to the required hardware and software to actively participate in e-learning activities.

5.2. Digital Citizenship: Students should demonstrate responsible digital citizenship by respecting intellectual property rights, adhering to acceptable use policies, and engaging in online discussions and collaborations in a respectful and ethical manner.

5.3. Time Management: Students should manage their time effectively, dedicating sufficient hours to studying, completing assignments, and actively participating in online discussions and activities.

5.4. Technical Support: Students should seek assistance from available technical support services to address any ICT-related issues they may encounter during their e-learning journey.

6. Support and Resources

6.1. Training and Professional Development: Faculty members should receive ongoing training and professional development opportunities to enhance their ICT skills and knowledge in e-learning methodologies, instructional design, and effective online teaching strategies.

6.2. Student Support Services: Adequate student support services, such as technical assistance, online tutoring, and academic advising, should be available to assist students in their e-learning endeavors.

7. Privacy and Data Security

7.1. Data Protection: Faculty members and students should adhere to the organization's data protection and privacy policies, ensuring the security and confidentiality of personal and sensitive information exchanged during e-learning activities.

7.2. Responsible Use: Faculty members and students should utilize ICT resources responsibly and follow the organization's acceptable use policies to maintain a safe and secure e-learning environment.

8. Policy Review

This policy will be periodically reviewed to ensure its effectiveness and alignment with technological advancements, best practices in e-learning ICT, and changing regulatory requirements.

Internet and Local Area Network Usage Policy

1. Introduction

This policy outlines the guidelines and responsibilities for the appropriate and responsible use of the Internet and Local Area Network (LAN) within the university. The purpose of this policy is to ensure secure and efficient utilization of network resources, promote ethical behavior, protect sensitive information, and maintain a productive and respectful digital environment.

1.1 Purpose:

The objective of the Internet Usage Policy is to establish guidelines regarding the maximum number of devices that users are allowed to connect to the university's network. The management of connected devices is crucial to maintain network performance, security, and accessibility. This policy aims to foster academic excellence and professional development while preventing network congestion, preserving network performance, and catering to the diverse requirements of its users.

1.2 Scope

This policy applies to all employees (faculty members and students of SIBAU) accessing the internet bandwidth and Local Area Network within the organization.

2. Acceptable Use

2.1 Authorized Users: This policy applies to all faculty members, students, staff, contractors, and any other individuals granted access to the university's network resources.

2.2 Educational and Work Purposes: Internet and LAN access provided by the university should primarily be utilized for educational, research, and work-related purposes in support of the institution's mission.

2.3 Compliance with Laws and Regulations: Users must comply with all applicable laws, regulations, and policies related to Internet and LAN use, including copyright laws, intellectual property rights, and data protection regulations.

2.4 Prohibited Activities: The following activities are strictly prohibited:

a) Unauthorized access or use of other users' accounts, data, or resources.
b) Intentional spreading of malware, viruses, or any other harmful software.
c) Engaging in activities that violate the privacy of others, such as unauthorized monitoring or interception of communications.

d) Accessing or distributing illegal, offensive, or inappropriate material.

e) Engaging in cyberbullying, harassment, or any form of discriminatory behavior.

f) Using the Internet and LAN for personal activities that are unrelated to educational or work purposes without proper authorization.

g) Any activity that disrupts or interferes with the normal operation of the university's network or systems.

3. Responsible Use

a. Faculty and staff members of Sukkur IBA University are permitted to simultaneously connect a maximum of five devices to the university's network using their user credentials. However, the specific limit on the number of devices allowed may vary depending on the individual's role, responsibilities, and anticipated data usage.

b. Students of Sukkur IBA University are allowed to connect up-to two devices to the university's network. However, the exact limit on the number of devices permitted may vary based on the Head of Department's request for semester projects assigned to the students.

c. Sukkur IBA University alumni will have the option to connect to the university's internet using their CMS IDs. Additionally, they will be able to access internet services across all universities in the country where HEC's "Eduroam" WIFI Internet is available.

d. Sukkur IBA University network will authenticate users' devices using CMS-ID and Password before connecting to the Sukkur IBA University Network. This provides an additional layer of security and ensures that only authorized users and devices can access the network.

e. Users will take necessary precautions to ensure the security of their accounts, passwords, and personal information. User will be solely responsible, if their IDs found in any cyber-attack or any anti institution cyber activity.

f. Sukkur IBA University reserves the right to adjust device limits or restrict access to certain users or groups of users as necessary to ensure the availability and performance of its network resources.

g. The ICT Department of Sukkur IBA University will actively monitor network traffic to ensure responsible and secure usage of the network. Any infringements on the university's internet and network policies may lead to disciplinary actions taken by the university.

3.1 Personal Responsibility: Users are individually responsible for their actions and behavior while using the Internet and LAN. They should exercise good judgment, professionalism, and ethical conduct.

3.2 Network Resource Conservation: Users should make efficient use of network resources and avoid excessive consumption of bandwidth, storage, or other network capacities that may negatively impact the overall performance for other users.

3.3 Protection of Credentials: Users must safeguard their usernames, passwords, and other login credentials. Sharing or providing access to university accounts or network resources to unauthorized individuals is strictly prohibited.

3.4 Reporting Security Incidents: Users should report any suspected security incidents, data breaches, or vulnerabilities promptly to the designated authorities or IT support team.

4. Network Monitoring and Security

4.1 Network Monitoring: The university reserves the right to monitor Internet and LAN traffic, access logs, and network usage for security, compliance, and network management purposes.

4.2 Security Measures: The university will implement appropriate security measures, including firewalls, intrusion detection systems, and antivirus software, to protect the network infrastructure and prevent unauthorized access or malicious activities.

4.3 Access Controls: Access to certain websites or network resources may be restricted based on security considerations or content filtering policies implemented by the university.

5. Policy Enforcement

5.1 Compliance and Disciplinary Actions: Violation of this policy may result in disciplinary actions, which can include warnings, temporary or permanent suspension of Internet and LAN privileges, and, in severe cases, legal consequences.

5.2 User Education and Awareness: The university will conduct regular user education and awareness programs to familiarize users with this policy, cybersecurity best practices, and their responsibilities in maintaining a secure network environment.

6. Policy Review
7. This Internet and LAN Usage Policy will be periodically reviewed to ensure its effectiveness, alignment with technological advancements, and compliance with legal and regulatory requirements.

SOCIAL MEDIA APPS POLICY

1. Introduction

1.1 Purpose: The purpose of this policy is to outline the guidelines and regulations regarding the use of social media apps on the university's internet network. This policy aims to ensure responsible and appropriate use of social media platforms by students, faculty, staff, and any other individuals accessing the university's internet services.

2. Scope: This policy applies to all users who access the university's internet network and utilize social media apps. It encompasses both personal and professional use of social media platforms while connected to the university's network.

3. Guidelines for Social Media Usage

3.1 Responsible Use: Users should exercise responsible and ethical behavior when using social media apps on the university's network. They should adhere to the university's code of conduct and policies while engaging in any social media activities.

3.2 Respect for Privacy and Confidentiality: Users must respect the privacy and confidentiality of others when using social media platforms. They should refrain from sharing sensitive information, personal data, or any content that violates privacy regulations or university policies.

3.3 Professional Conduct: Users representing the university on social media platforms should maintain professionalism and adhere to the university's branding guidelines. They should avoid engaging in online activities that may harm the university's reputation or violate any ethical standards.

3.4 Compliance with Laws and Regulations: Users must comply with all applicable laws and regulations while using social media apps on the university's network. They should refrain from engaging in any activities that may be illegal, defamatory, or infringe upon intellectual property rights.

3.5 Appropriate Content: Users are responsible for ensuring that the content they post or share on social media platforms aligns with the university's values and policies. They should avoid posting offensive, discriminatory, or inappropriate content that may be harmful to individuals or groups.

3.6 Security Measures: Users should take necessary precautions to protect their social media accounts and prevent unauthorized access. This includes using strong passwords, enabling two-factor authentication, and keeping their accounts updated with the latest security features.

3.7 Monitoring and Enforcement The university reserves the right to monitor social media activities conducted on its network for compliance with this policy. Any violations may result in disciplinary actions, including but not limited to warnings, account suspensions, or termination of network access privileges. The severity of the consequences will depend on the nature and extent of the violation. **Users who violate this policy may face disciplinary action, such as warnings, fines, or other restrictions**.

3.8 During office hours, access to social media applications such as Facebook, Instagram, YouTube, Netflix, and other similar apps will be restricted on the university's network for all students, faculty, and staff.

3.9 The ICT Department will authorize access to social media apps for academic or research purposes during office hours based on recommendations from the Heads of Departments.

4. To ensure optimal network speed and efficient utilization, individual users will be subject to internet capping. Faculty and staff members will have a limit of 4 Mbps assigned to each ERP-ID, while students' CMS-IDs will be capped at 2 Mbps. However, departments or individuals responsible for managing the institution's digital media may be granted higher bandwidth allocation, as per the recommendations of their respective department heads.

5. By adhering to this policy, users contribute to maintaining a positive and respectful online environment while utilizing social media apps on the university's internet network.

6. Policy Review: This policy will be reviewed periodically to ensure its effectiveness and alignment with changing technologies and social media trends. Updates to the policy will be communicated to all users, and their compliance will be expected.

GOOGLE WORKSPACE (EMAIL DOMAIN) POLICY

1. **Introduction**

1.1 Purpose: This Email Usage Policy outlines guidelines and expectations for the use of email within SIBAU. It aims to promote effective communication, ensure the security and confidentiality of information, and maintain a professional image for the organization.

1.2. Scope:This policy applies to all authorized users [Faculty/Staff, staff, and student] who have access to the email system provided by SIBAU. It covers all email messages, attachments, and related content transmitted or received through the organization's email system.

2. **Acceptable Use**

2.1. Professional Communication: All email communications should adhere to professional standards. Users are expected to use appropriate language, maintain a respectful tone, and employ proper grammar and punctuation. Slang, offensive or discriminatory language, and unprofessional content are strictly prohibited.

2.2. Clear and Concise Subject Line: Emails should have a clear and concise subject line that accurately reflects the content of the message. This helps recipients understand the purpose of the email and allows for efficient organization and retrieval of emails.

2.3. Use of Organizational Email for Official Communication: Organizational email accounts should be used for official business purposes only. Personal use should be limited and conducted during non-working hours. Users must remember that organizational email is subject to monitoring and should not be used for personal or illegal activities.

2.4. Data Protection and Confidentiality: Users must exercise caution when sending emails to protect sensitive information. Confidential and proprietary information should only be shared with authorized recipients. Users should avoid forwarding or sharing emails containing confidential information without proper authorization.

3. Prohibited Actions

3.1. Spam and Unsolicited Email: Sending unsolicited email, chain letters, or spam is strictly prohibited. Users should not forward or reply to spam emails and should report such incidents to the ICT department.

3.2. Malicious Content and Viruses: Users must not send or open emails that contain malicious content, viruses, or harmful attachments. It is essential to maintain up-to-date antivirus software and exercise caution when opening attachments or clicking on links.

3.3. Impersonation and Fraudulent Activities: Impersonating other individuals or entities, forging email headers, or engaging in any fraudulent activities through email is strictly prohibited.

3.4. Email Etiquette: Users are expected to follow email etiquette guidelines, including being courteous, responding promptly, and using "Reply All" judiciously. Large attachments should be compressed or shared through alternate file-sharing methods to avoid email system overload.

4. Monitoring and Enforcement

4.1. Monitoring The organization reserves the right to monitor email usage to ensure compliance with this policy, maintain system performance, and investigate any suspected violations or security breaches.

4.2. Compliance Failure to comply with this policy may result in disciplinary action, including verbal or written warnings, temporary or permanent suspension of email privileges, and, in severe cases, termination of employment or legal action, depending on the nature and severity of the violation.

5. Policy Review

This policy will be reviewed periodically by the SIBAU, ICT department to ensure its relevance and effectiveness. Any necessary updates or revisions will be communicated to all users.

6. Conclusion:

By adhering to this Email Usage Policy, users contribute to maintaining professional communication standards, protecting organizational information, and promoting effective collaboration within SIBAU.

POLICY FOR EMAIL ADMINISTRATORS:

1. Introduction

1.1. Purpose:

This Email Administrators Policy establishes guidelines and responsibilities for individuals designated as Email Administrators within SIBAU. It outlines the proper management, maintenance, and security measures related to the organization's email system.

1.2. Scope:

This policy applies to all Email Administrators who are responsible for the administration, configuration, and maintenance of the email infrastructure within SIBAU.

2. Roles and Responsibilities

2.1. Email System Administration:

Email Administrators are responsible for the administration and configuration of the organization's email system, including user accounts, distribution lists, email security settings, and mailbox quotas. They must ensure that the email system functions properly and meets the organization's communication needs.

2.2. User Account Management:

Email Administrators are responsible for creating, modifying, and disabling user accounts as per authorized requests. They must follow proper procedures for account provisioning, ensuring that user access privileges align with their roles and responsibilities within the organization.

2.3. Email Security and Compliance:

Email Administrators play a crucial role in maintaining email security and compliance. They are responsible for implementing and enforcing security measures, such as spam filters, antivirus protection, and encryption protocols. They must also stay updated with relevant laws, regulations, and industry best practices related to email communication and data privacy.

2.4. System Maintenance and Upgrades:

Email Administrators are responsible for performing regular system maintenance tasks, including software updates, patches, and system backups. They should coordinate with the ICT department to ensure minimal disruption to email services during maintenance activities.

2.5. User Support and Training Email:

Administrators should provide technical support to users regarding email-related issues, including troubleshooting problems, assisting with email client configurations, and guiding users on best practices for email usage. They may also conduct training sessions or provide documentation to help users optimize their email experience and adhere to the organization's email policies.

3. Security and Confidentiality

3.1. Data Protection Email:

Administrators must ensure the confidentiality and integrity of email data within the organization. They should implement appropriate security measures to protect against unauthorized access, data breaches, and other security threats.

3.2. Access Control Email:

Administrators should adhere to access control procedures and ensure that only authorized personnel have administrative privileges for the email system. They should enforce strong password policies and regularly review access rights to prevent unauthorized access to sensitive information.

4. Compliance and Monitoring

4.1. Policy Compliance:

Email Administrators are expected to comply with all relevant organizational policies, including email usage policies, data protection policies, and IT security policies. They must ensure that email system configurations and practices align with these policies.

4.2. Monitoring and Auditing:

Email Administrators may be required to monitor email system usage, perform periodic audits, and generate reports on system performance, security incidents, and compliance. They should promptly report any policy violations or security breaches to the appropriate authorities.

5. Policy Review

This policy will be reviewed periodically by the ICT department to ensure its relevance, effectiveness, and compliance with changing technological and regulatory requirements. Any necessary updates or revisions will be communicated to all Email Administrators.

6. Conclusion

By fulfilling their roles and responsibilities as Email Administrators in accordance with this policy, individuals contribute to the secure and efficient operation of the organization's email system. Their efforts ensure reliable communication, safeguard sensitive information, and maintain compliance with applicable regulations and policies.

NEW USER AND PASSWORDS POLICY:

1. Introduction

1.1. Purpose The New Email User and Password Policy establishes guidelines and procedures for the creation and management of email user accounts and passwords within SIBAU. This policy aims to ensure the security, confidentiality, and proper administration of email accounts for all authorized users.

1.2. Scope:

This policy applies to all Faculty/Staff, contractors, and authorized users who require access to the organization's email system provided by SIBAU.

2. Account Creation

2.1. Account Request Process New users requiring an email account must follow the designated account request process established by the ICT department. This typically involves submitting a formal request, providing necessary details, and obtaining proper authorization.

2.2. Authorized Account Creation:

Email accounts will only be created for individuals who have a legitimate need for email access based on their roles, responsibilities, and affiliation with SIBAU. Account creation will be approved by the appropriate authority.

2.3. Account Naming Convention:

Email account usernames will follow a standardized naming convention to ensure consistency and ease of identification. The ICT department will provide guidelines regarding the naming format to be used.

3. Password Management

3.1. Strong Passwords All users are required to create strong and secure passwords for their email accounts. Passwords must meet the organization's password complexity requirements, which may include a minimum length, a combination of uppercase and lowercase letters, numbers, and special characters.

3.2. Password Confidentiality Users must keep their email account passwords confidential and not share them with others. Passwords should not be written down or stored in an easily accessible location.

3.3. Password Change and Reset:

Users should periodically change their email account passwords as per the organization's password policy. The ICT department may also require password resets in case of suspected security breaches or compromised accounts.

4. Account Deactivation and Termination

4.1. Account Deactivation Email accounts of users who leave SIBAU. or no longer require email access will be deactivated promptly. The HR department or appropriate authority must inform the ICT department of any employee terminations or changes in access requirements.

4.2. Account Data Retention:

Upon account deactivation or termination, the ICT department will ensure that appropriate measures are taken to retain or securely delete any email data associated with the deactivated or terminated account in accordance with applicable data protection regulations and organizational policies.

4.3. Security and Compliance

Access Control Access to email accounts is limited to authorized users only. Users must not share their email account login credentials with others and should take appropriate measures to protect their accounts from unauthorized access.

4.4. Monitoring and Auditing:

The ICT department may monitor email system usage, including user login activities, for security and compliance purposes. This monitoring helps detect and prevent unauthorized access, identify potential security breaches, and ensure adherence to organizational policies.

5. Policy Review

This policy will be reviewed periodically by the ICT department to ensure its relevance, effectiveness, and compliance with changing technological and regulatory requirements. Any necessary updates or revisions will be communicated to all users.

6. Conclusion

By adhering to the guidelines and procedures outlined in this new Email User and Password Policy, users contribute to the security and effective management of email accounts within SIBAU. It ensures the protection of sensitive information, promotes secure communication, and supports compliance with applicable policies and regulations.

RECEIVING AND POSTING OFFICIAL EMAILS ON GROUPS (FACULTY, STAFF AND STUDENTS) POLICY:

1. Introduction

1.1.1. Purpose:

The Posting and Receiving Official Emails for Faculty, Staff and Students on Groups Policy establishes guidelines and procedures for the posting and receiving of official emails within designated groups by Faculty, Staff and Students of SIBAU. This policy aims to ensure efficient communication, collaboration, and information sharing within the organization's official email groups.

1.1.2. Scope:

This policy applies to all Faculty, Staff and Students of SIBAU. who have access to the organization's official email system and are members of designated official email groups.

1.2. Posting Official Emails on Groups

1.3. Purpose and Relevance:

Official emails posted on groups should be directly related to the objectives, activities, or announcements of the designated group. Only emails that are of significance and relevance to the group's members should be posted.

1.4. Group Communication:

Guidelines When posting official emails on groups, users should adhere to the following guidelines:

I. Clearly indicate the purpose of the email in the subject line.
II. Use a professional and respectful tone in the email content.
III. Ensure that the email provides accurate and necessary information to the group members.
IV. Avoid excessive or unnecessary attachments unless required for the group's activities.
V. Follow the organization's email formatting and style guidelines, if applicable.

2. Approval Process:

Some official emails may require approval from designated authorities (HoDs/Sectional heads) before being posted. The approval process, if applicable, should be clearly communicated within the group and followed accordingly.

3. Receiving Official Emails on Groups

3.1. Active Participation Group members are responsible for actively monitoring and checking emails posted on the official groups they are part of. Regularly reviewing and staying updated with the posted emails is essential for effective communication within the group.

3.2. Email Response Etiquette:

When responding to official emails on groups, users should adhere to the following guidelines:

a. Respond in a timely manner, especially if the email requires a response or action.

b. Use a professional and respectful tone in email responses.

c. Keep responses concise and relevant to the topic.

d. Avoid unnecessary "reply all" responses unless it adds value to the discussion or is essential for information sharing.

4. Confidentiality and Data Protection

4.1. Data Sharing and Confidentiality Group members should respect the confidentiality of information shared within the official email groups. Confidential or sensitive information should only be communicated within the group when necessary and in accordance with the organization's data protection and confidentiality policies.

4.2. Unauthorized Sharing Group members should refrain from sharing or forwarding official group emails to unauthorized individuals or external parties without proper authorization. Email content should remain within the intended audience of the group.

5. Policy Compliance and Violations

5.1. Compliance Monitoring:

The ICT department or designated authorities (HoDs/Sectional heads/Directors) may periodically monitor the posting and receiving of official emails on groups to ensure compliance with this policy.

5.2. Violations:

Any violations of this policy, including inappropriate or unauthorized use of official group emails, should be reported to the appropriate authority for investigation. Violations may result in disciplinary action in accordance with the organization's policies and procedures.

6. Policy Review

This policy will be reviewed periodically by the ICT department or designated authority to ensure its relevance, effectiveness, and compliance with changing technological and regulatory requirements. Any necessary updates or revisions will be communicated to all staff and students.

7. ***Note:*** ***The Head of Department has the authority to request the inclusion of names for granting posting rights for sending emails.***

8. Conclusion

By following the guidelines and procedures outlined in this Posting and Receiving Official Emails for Faculty, Staff and Students on Groups Policy, individuals contribute to effective communication, collaboration, and information sharing within the organization's official email groups.

Note: Below are some existing email groups that are currently operational within the university for reference:

1. faculty@iba-suk.edu.pk: The faculty email group is specifically designated for teaching/faculty members, while the departmental email group is meant to receive the emails. Only Heads of Departments (HoDs) and departmental coordinators will be granted the privilege to post emails. Furthermore, it is recommended to contemplate extending the posting rights to HoDs and higher authorities.
2. staff@iba-suk.edu.pk: The administrative email group is exclusively reserved for non-teaching staff members of SIBAU, while the administrative-related email group is intended to receive the emails. Only HR, Registrar, Directors, Sectional Heads and VC secretariat will have the privilege to post emails. Additionally, it is advisable to consider extending the posting rights to higher authorities.
3. students@iba-suk.edu.pk: The email group will exclusively consist of students or student batch email groups for receiving emails.
4. hods@iba-suk.edu.pk: The email group will only have Head of Department (HoDs) receiving and sending the emails.

5. sectional.heads@iba-suk.edu.pk email group will only have sectional heads receiving and sending the emails.
6. There will be a separate email group for the gazette officers (BPS 17 and above) staff members as officers@iba-suk.edu.pk.
7. No email ID will directly be added in the main groups like students, staff, or faculty instead those will be added in the relevant departmental email groups which eventually are added in the main groups of students, staff and faculty. For example: email group of departments of Computer Science is faculty.cs@iba-suk.edu.pk

Note: This policy will be reviewed periodically by the Higher Authorities and university administration to ensure its effectiveness and relevance. Any necessary updates or amendments will be communicated to the email groups members in a timely manner.

Relieving of an employee/passing out of student batches:

8. HR Department will notify the Email Administrator about the status of the Faculty/Staff as being on lien, on study leave or as resigned at the time of relieving.
9. Whenever an employee goes for study leave his/her email id will be removed from relevant departmental email group and will be added in the scholars' email group.
10. Email IDs of Faculty/Staff on lien will be removed from all email groups and will remain active for up to 3 years.
11. Whenever an employee resigns from the university his/her email account will be suspended after one year of resignation in order to facilitate him/her to back up his/er data to alternative locations.
12. Whenever the batches of students pass out, then after six months of the passing out their batch email groups will be removed from students' group and will be added in the Alumni email group by Email Administrator or Group Managers.

13. Whenever an employee resigns from the university and he/she is also the alumnus of SIBAU and was using the same student ID during the tenure of employment then his/her email ID will be removed from all the departmental email groups and will remain only the member of Alumni Email Group. If he/she was using or was, allotted new email id other than student ID then **point 17** will be applicable.

Group Managers:

14. Students and Alumni Affairs Office working at Career Development Center will be made managers of Students and Alumni Email groups to add or remove the members as per policy from the email groups.
15. Manager or Owner Rights of the email group will only be assigned to the users who need to add or remove the users from the group by themselves with the approval of HOD. For example: HOD in case of departmental email group and Alumni Affairs Office in case of Alumni or Students email groups.

Email and Google Drive Storage Policy

16. The students and alumni email groups will have a storage capacity of 25 GB, while staff members will be allocated a limit of 50 GB, and faculty members will have access to 100 GB of storage. In case additional space is required, it can be exclusively provided based on the recommendation of higher authorities.
17. All those email IDs will be deleted who have never signed in their accounts since their creation and within six months period.
18. All those email IDs will be deleted who have not signed in for last three years.
19. If Email IDs are in suspended status, then those email IDs will be deleted after one year of their suspension.
20. This policy will be reviewed and updated as necessary to ensure its continued effectiveness and relevance to our organization.

CMS (CAMPUS MANAGEMENT SOLUTION)

Student CMS IDs Creation:

1. Admission Department will provide the list of admitted students with detailed information to the ICT department.
2. CMS Personals will process the above list and create the CMS IDs, User Profiles, LDAP Accounts and Email Addresses.
3. After processing the mentioned list by performing above activities, the processed list will again be shared with Admission Department.
4. Admission Department will convey to the concerned Departments and students.

Course Scheduling: (Class Numbers Creation)

1. The CMS Personals will share the template files with all departments to fill out the required course detail information for that particular term.
2. The concern departments will provide the course catalogue numbers, semester, section wise with teacher information to CMS Personals.
3. CMS Personals will process the above said list of courses by creating the class numbers and teaching assignment.

Enrollment

1. The concern departments will provide CMS personals the new and existing list of students' section wise for enrollment.
2. CMS personals will process the above lists for enrollment.
3. After the enrollment, the attendance rosters will be created.
4. The Attendance of the courses will automatically be locked after the date changes and faculty will not be able to update.

- If faculty member wants to update any student attendance, the department will forward an email to CMS personals and from CMS personals the attendance update will take place.

5. In case of back date attendance faculty has two options:
    - The faculty member will be able to take back date attendance, but will not be able to update.
    - The faculty member will take back attendance in future dates in which there is no any class scheduled for that course.

Course Grade-book Lock and Unlock

1. If the faculty member pressed / clicked the lock button at grade-book unintentionally then they will have to send the email to Examination department to unlock it.
2. If the faculty member wants the course grade-book to unlock, he / she will have to email the Examination Department for acknowledgement / permission to unlock.
3. If examination department acknowledge then, CMS Personals will unlock the course grade-book.
4. For practical courses, the final category will be unlocked for the faculty members.
5. For Masters / Ph.Ds. final category will also be unlocked.

CMS IDs Passwords Reset:

If students want to reset their passwords, then they will have to follow the self-service password reset steps shared with them via email by CMS Office.

Employee on leave / terminate / resign / study leave.

i. The HR Department provides the detail about the employee to CMS Personals.

ii. If employee is terminated or he/she has resigned or on leave (with or without pay) then CMS personals block the CMS ID.

LDAP Accounts

1. LDAP accounts will be created at the time of Students induction.
2. LDAP accounts for faculty / staff / administrative officials will be created at the time of CMS ID creation when an employee joins the university.

POLICY: PRINTING PAPERS AND PHOTOCOPIES

1. Introduction

This policy outlines the guidelines and procedures for the responsible use of printing papers and photocopies within the organization. The purpose of this policy is to promote efficient resource utilization, reduce waste, and encourage environmentally friendly practices.

2. Scope

This policy applies to all Faculty/Staff, contractors, and authorized personnel who have access to the organization's printing and photocopying facilities.

3. Responsible Use of Printing Papers

3.1 Digital Documentation: Whenever possible, Faculty/Staff are encouraged to utilize electronic formats for documentation, such as email, digital files, and online collaboration tools, to minimize the need for printing papers.

3.2 Printing Necessity: Faculty/Staff should exercise discretion and consider the necessity of printing before initiating print jobs. Printing should be limited to situations where a hard copy is required for legal, official, or essential purposes.

3.3 Duplex Printing: Duplex printing (printing on both sides of the paper) is encouraged to reduce paper consumption. Printers and copiers should be set to default duplex printing mode, unless single-sided printing is necessary.

3.4 Draft Printing: For internal documents that do not require high-quality printing, Faculty/Staff should utilize draft or grayscale printing settings to conserve ink and toner.

3.5 Font and Formatting: Efficient use of printing papers can be achieved by selecting appropriate font types, sizes, and spacing that minimize the number of pages needed for a document.

4. Photocopying Guidelines

4.1 Original Document Assessment: Before making photocopies, Faculty/Staff should evaluate whether a copy is necessary or if alternative methods, such as scanning or digital sharing, can serve the purpose.

4.2 Single-sided versus Double-sided: Similar to printing, double-sided photocopying is encouraged to conserve paper resources. Faculty/Staff should ensure that default settings on photocopiers are set to double-sided copying.

4.3 Quantity Consideration: Faculty/Staff should assess the number of copies needed and avoid excessive photocopying. When feasible, Faculty/Staff are encouraged to share documents digitally or print a single copy for reference and utilize shared document centers. Academic and administrative documents will be printed with the approval of concerned Head of departments, Sectional Heads and higher authorities.

5. Recycling and Waste Reduction

5.1 Recycling Bins: Clearly labeled recycling bins should be provided near printing and photocopying stations for Faculty/Staff to dispose of used papers. Faculty/Staff should be educated on the importance of paper recycling and encouraged to utilize the recycling bins appropriately.

5.2 Paper Waste Reduction: Faculty/Staff should strive to minimize paper waste by utilizing scrap paper or using blank sides of used papers for internal printing or note-taking purposes, whenever appropriate.

5.3 Responsible Disposal: Confidential or sensitive documents should be shredded before disposal to maintain data security and protect sensitive information.

6. Compliance and Accountability

6.1 Compliance: All Faculty/Staff and authorized personnel are expected to adhere to this policy. Failure to comply with the guidelines outlined may result in corrective action, including counseling or disciplinary measures.

6.2 Reporting Violations: Faculty/Staff should report any observed violations or instances of excessive paper waste to the designated authority or the environmental sustainability team.

7. Awareness and Training

7.1 Communication: This policy will be communicated to all Faculty/Staff through appropriate means, such as campus-wide emails, staff meetings, and employee handbooks.

7.2 Training: Faculty/Staff will receive training on responsible printing and photocopying practices during orientation sessions and as part of ongoing sustainability training programs.

Review and Revision

This policy will be periodically reviewed and revised as necessary to ensure its effectiveness and alignment with changing environmental regulations, industry best practices, and organizational needs.

Campus CCTV Surveillance Policy

1. Introduction

   This policy outlines the guidelines and regulations regarding the use of Closed-Circuit Television (CCTV) surveillance on campus. The purpose of this policy is to ensure the safety and security of individuals, protect campus property, and maintain a conducive environment for learning and working.

2. Scope

   This policy applies to all members of the campus community, including students, faculty, staff, visitors, and any other individuals present on campus premises.

3. Purpose of CCTV Surveillance

3.1. Deterrence and Prevention: The presence of CCTV cameras acts as a deterrent against criminal activities, promoting a safer campus environment and reducing the likelihood of incidents.

3.2. Investigation and Evidence: CCTV footage may be used as evidence for investigating criminal activities, violations of campus policies, or any other incidents that may occur on campus.

3.3. Emergency Response: CCTV surveillance aids in monitoring and responding to emergencies promptly, ensuring the safety and well-being of individuals.

4. Placement and Operation of CCTV Cameras

4.1. Strategic Placement: CCTV cameras will be strategically located across campus to maximize coverage of critical areas, such as entrances, exits, parking lots, common areas, and high-security zones.

4.2. Privacy Considerations: Privacy concerns will be taken into account when determining the placement and coverage of CCTV cameras. Areas where individuals have a reasonable expectation of privacy, such as restrooms, changing rooms, and private offices, will not be monitored.

4.3. Camera Operation: CCTV cameras will operate 24/7, continuously recording footage for a predetermined retention period. The campus security team will be responsible for monitoring the cameras and reviewing the footage as necessary.

4.4. Camera Visibility: The presence of CCTV cameras will be clearly indicated through signage to inform individuals that they are under surveillance.

5. Access to CCTV Footage

5.1. Authorized Personnel: Access to CCTV footage will be limited to authorized personnel, including campus security staff and designated administrators responsible for investigating incidents or reviewing footage.

5.2. Data Protection: Access to CCTV footage will be protected and strictly controlled to prevent unauthorized use, disclosure, or tampering. Proper security measures, including user authentication and encryption, will be implemented to safeguard the footage.

5.3. Retention Period: CCTV footage will be retained for a specified period, based on legal requirements and campus policies. Once the retention period expires, the footage will be securely erased, unless it is required for ongoing investigations or legal proceedings.

6. Compliance and Accountability

6.1. Compliance: All individuals on campus must comply with this CCTV surveillance policy. Deliberate interference with CCTV cameras, unauthorized access to footage, or any other misuse of the surveillance system may result in disciplinary action.

6.2. Policy Review: This policy will be periodically reviewed to ensure its effectiveness and alignment with relevant laws and regulations.

6.3. Grievances and Concerns: Individuals who have concerns or grievances regarding the use of CCTV surveillance should follow the appropriate channels to report their concerns to the campus security office or designated authorities.

7. Awareness and Communication

7.1. Notification: The campus community will be notified of the presence and purpose of CCTV surveillance through appropriate means, such as campus-wide announcements, signage, and the institution's website.

7.2. Education and Training: Training programs will be conducted to educate the campus community about the CCTV surveillance policy, including the purpose, guidelines, and their rights and responsibilities.

7.3. Transparency: The campus administration will ensure transparency by providing information about the CCTV surveillance system, its purpose, and how it aligns with privacy laws and regulations.

8. Revision and Approval

This policy will be reviewed and revised as necessary by the higher authorities of SIBAU and relevant committee members to ensure its continued effectiveness and compliance with changing needs and legal requirements.

Datacenter Policy

The ICT Data Center is an indispensable aspect of Sukkur IBA University's information technology operations. To ensure the continued security, availability, complexity, and reliability of the systems and network housed within the center, comprehensive policies have been developed. It is imperative that all individuals who access the ICT Data Center understand, agree with, and comply with these policies.

Purpose and Objectives: The purpose of this section is to provide guidelines and procedures relating to access control, environmental control, and operations of ICT Data Centre.

Scope: This policy applies to all faculty, staff, and students of SIBAU.

1. Physical Security: The datacenter will be physically secure, and access will be restricted to authorized personnel only. The datacenter will be equipped with video surveillance cameras, and fire alarms. The datacenter will also have appropriate environmental controls, such as temperature and humidity monitoring, to ensure the safety of equipment.

2. Access Control: Access shall be controlled via Biometrics fingerprint devices and all doors shall be fitted with sensors to detect unauthorized or prolonged opening. Only authorized ICT Data center and Network team personnel shall have access to the Data Centre via the biometrics devices. Any other personnel including full time Faculty/Staff, contractors and vendors shall be escorted by authorized ICT Data center and/or Network team during office hours.

3. Network Security: All network devices shall be secure with strong passwords, and passwords must be changed on regular basis. Network devices shall be updated with the latest security patches and firmware updates. Network traffic shall be monitored to detect and prevent security threats. Firewalls shall be used to restrict access to the datacenter network, and only authorized ports and protocols shall be allowed.

4. UPS Provisioning: All equipment at the Data Centre shall be powered on by a UPS system, the UPS system shall sustain power to those devices for at least 15 minutes to allow graceful shutdown. Service shall be done at least annually by a reputable maintenance service provider as per recommended by Electrical Engineering Department

5. Monitoring: Data Center Infrastructure Management software shall be deployed / installed for infrastructure management. The ICT datacenter shall be monitored 24/7 through a combination of security CCTV cameras, and other monitoring tools.

6. Air Conditioning: INROW Precision cooling solution shall be provided in the Data Centre. It shall deliver enough cooling per rack in accordance with design specification. Service shall be done at least three times a year by Electrical Engineering Department and a reputable maintenance service provider. A service health certificate shall be maintained in Department.

7. FM-200 Fire Extinguisher: FM-200 fire suppression system shall be provided in the Data Centre. Service shall be done at least annually by a reputable maintenance service provider for FM-200 fire suppression shall be done. A service health certificate shall be maintained in Department.

8. Change and Configuration Management: The Senior Data Center Engineer shall be responsible for all changes that shall take place at the Data Centre. All changes to be made shall be requested to and authorized by the Director ICT. The Sr. Data Center Engineer will monitor and review the Data Centre access logbook on a regular basis.

9. Waste Disposal and Cleaning: Cardboard and other items that can generate dust and that are easily combustible shall remain outside the Data Centre. Waste bin shall be available outside the Data Centre main entrance for easy disposal of other items of waste.

10. Dust Prevention: The Data Centre shall be well ventilated to prevent dust from affecting equipment. Equipment to be installed in the Data Centre shall be dust freed outside before introduced.

11. Training and Awareness: All personnel who have access to the datacenter should receive regular security and maintenance awareness training to ensure that they are aware of potential security threats and best practices for mitigating them.

12. Cables and Wiring: Cables and wires shall be structured and labelled and should be properly placed in running ceiling mounted trays, and equipment racks.

13. List of Prohibited Items: Combustible materials such as paper and cardboard, food and drink, tobacco products, explosives and weapons, hazardous materials, alcohol, illegal drugs and other intoxicants, electro-magnetic devices that could cause interference with computer and telecom equipment, radioactive materials, photographic or recording equipment.

14. Electrical Safety: Only qualified electrical technicians shall have access to electrical systems, ICT staff and other personnel should contact the relevant electrical personnel when encountering electricity problems.

15. Hours of Operation: The Data Centre will be operated during office hours to authorized personnel between 9:00AM to 5:00PM. Access afterhours for maintenance purposes will be authorized and delegated by the Sr. Data Center Engineer.

16. Equipment delivery & deployment: Delivery and deployment of equipment shall be supervised by authorized personnel upon approval by the Senior Sr. Data Center Engineer.

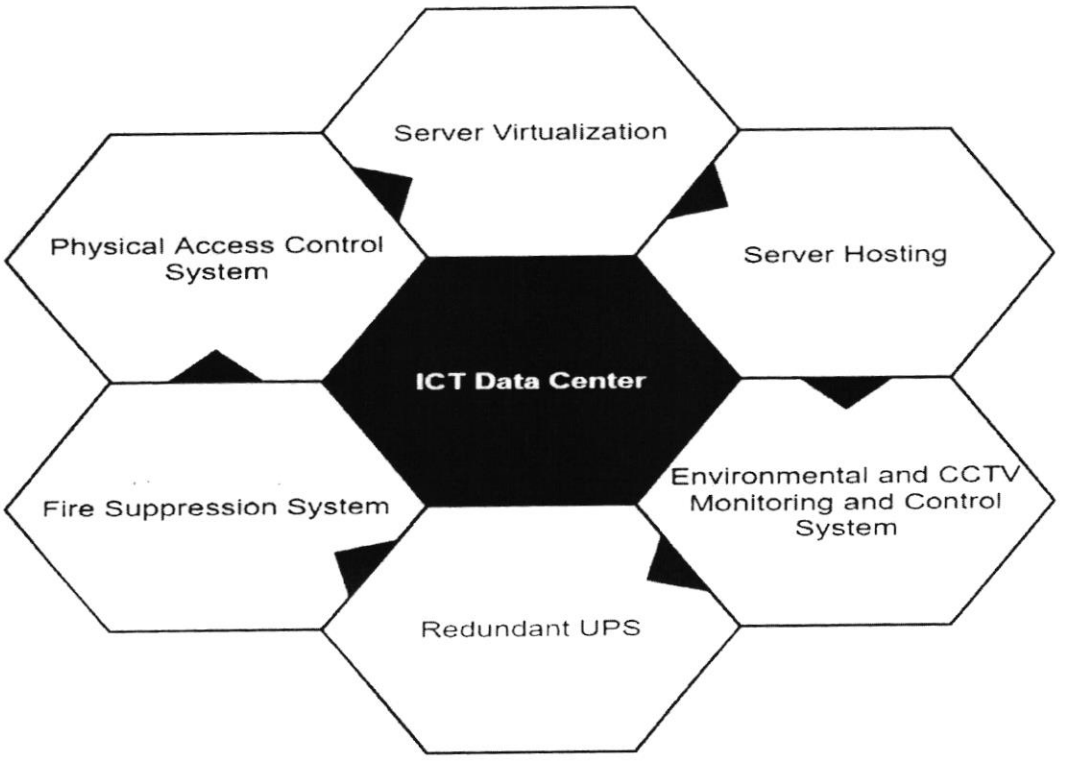
17. Data Security & Backup appliances / hardware and software: Data security and backup appliance / hardware and software shall be deployed in data center for data protection.

18. Faulty Equipment Replacement: **The faulty equipment replacement will be provided.**

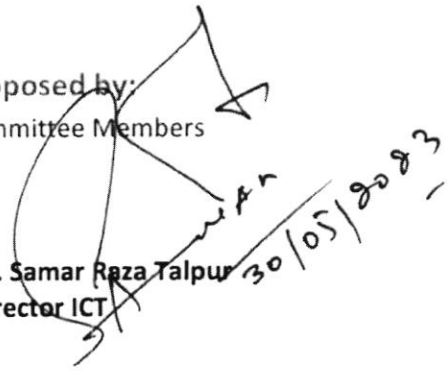
19. End of Life Equipment: **End of Life equipment will be replaced as per IT standard and policies 3 to 5 years.**

20. Control of Equipment: **No unused equipment and spares shall be left at the Data Centre.**

Data center Salient Features Layout



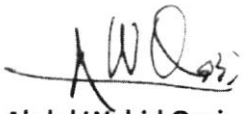
Proposed by:
Committee Members



Dr. Samar Raza Talpur
Director ICT

Prof. Dr. Sher M. Daudpota
Director QEC

Prof. Dr. G. Mujtaba Shaikh
Director CRAIB LAB



Abdul Wahid Qazi
Director CDC

Reviewed by:

Approved

Azhar Ali Soomro
Registrar

Prof. Dr. Asif Ahmed Shaikh
Vice Chancellor