Primary Access Policies for IT

Access to privileged user accounts

Following table lists user IDs for important devices and services and the officials, who have access to password of IDs.

Devices and Services	**User accounts**	**Access to Password**
All network Switches, SAN switch, Core switch	Radius	Manager AM (SA&N)
Servers (Active Directory, DHCP, File server, and edu.in DNS)	Administrator	Manager AM (SA&N) Technical Assistant
Firewall (Fortinet)	Admin	Manager AM (SA&N)
	support	Chair IT Committee Manager AM (SA&N)
WiFi controller	admin	Manager AM (SA&N) Technical Assistant
Web Server (edu.in)	root	Chair IT Committee Manager AM (SA&N)
backpack	Administrator & Individuals	BackPack Admin
Lab PCs	Administrator	Manager AM (SA&N) Technical Assistant
Web and external DNS	admin	Webadmin AM (SA&N)
ERP	Application login	Manager academic AM (SA&N)
	Server login	

HPC		Manager AM (SA&N)
Storage and NAS		Manager AM (SA&N))
VMware blade server		Manager AM (SA&N)
Library server		Manager AM (SA&N)
All IT department VMs and licence servers		Manager AM (SA&N) Technical Assistant
IP EPABX and analog gateways		Manager AM (SA&N) Technical Assistant
Google Apps (mailing server)		Chair IT Committee Manager AM (SA&N)

Currently, following are the officials.

- Chair IT Committee: Dr. Sambuddho Chakravarty
- Google Apps Admin: Dr. Sambuddho Chakravarty
- Backpack Admin: Apoorv Narang and Apoorv Singh
- Webadmin : Ankit Agarwal
- AM (SA&N): Adarsh, Bhawani, Yogesh, Rahul
- Senior Manager: Mr. Abhinay Saxena
- Technical Assistants: Mr. Binod, Shailendra

The Director can ask for password of any user account.

Escalation sequence

It is mentioned here http://it.iiitd.edu.in/static/Escalation.htm

Creating email IDs in ac.in domain

IIIT-D email ID is issued to all the students, office staff, and faculty. For visiting faculty, visiting students, or research associates, email IDs will be provided if they are visiting us for at least a semester. If they prefer, their non-IIIT-D email IDs can be added to relevant aliases/groups of IIIT-D. Followings are the rules to assign IDs.

- BTech: First Name followed by 2-digit enrollment year and 3 digits of roll number
  Example: richa10060@iiitd.ac.in
- MTech: First name followed by 2-digit enrollment year and 2 digits of roll number
  Example: richa1060@iiitd.ac.in
- PhD: First name followed by initial of the last name
  Example: richas@iiitd.ac.in
- Office: First name if avaialable, if not then first name followed by initial of the last name
  Example: richa@iiitd.ac.in
- Faculty: According to their choice and availability
  Example: rsingh@iiitd.ac.in

Following are the permissions required for creation of email IDs

- For student ID, the concerned (UG/PG) Chair requests to corresponding Admin
- For staff ID and faculty, the HR Manager requests to corresponding Admin
- For RA, the faculty hiring the RA requests to corresponding Admin
- The Director can issue a request for any ID to corresponding Admin

Creating firewall and active directory IDs

Same as that of Creating email IDs in ac.in domain but the domain name is replaced by edu.in

Managing email, firewall, and active directory IDs

- Resetting of passwords
  - The requester has to authenticate himself/herself to the corresponding Admin for resetting password of his/her own ID, preferably institute issued ID card.
- Deletion of IDs
  - For departure from the institute, this policy will apply
  - For the IDs of the students, who have left the institute prior to completion of course, will be deleted.
  - The Director can issue a request for deletion of any ID to corresponding Admin
- Suspension of IDs
  - For student ID, the concerned (UG/PG) Chair or Disciplinary Action Committee Chair or IT Committee Chair requests suspension to corresponding Admin
  - For staff ID, the staff Manager requests suspension to corresponding Admin
  - The Director can issue a request for suspension of any ID to corresponding Admin

Creating lists/groups in IIIT-D domain

The lists/groups feature of Google Apps is to facilitate sending emails to a group of people efficiently. Following are the guidelines for creating email alias or groups.

- A lists/group should represent a logical group that
  - Consists of more than five members
  - The lists/groups needs to be accessed frequently and accessing all the members together is important
  - The lists/groups will last for a long time (otherwise the users can create alias using their email id itself)
  - The Google Apps Admin will assign an owner(s) to the lists/groups.
- A lists/group should only contain the members of that logical group only and all members of that logical group should be included in the list.
- The owner(s) of each lists/group decides its policy for posting to it, having members from IIIT-D domain or outside the domain, and about the post visible to members of the list only/members of the domain. However, the membership of all lists should be visible to all members of IIIT-D.
- The Director, Deans, and the IT Committee Chair will have posting permission to all the lists/groups
- Lists/groups can be generated for courses that have students enrolled from multiple batches. These lists/groups will be deleted once the course grades are finalized, i.e., two weeks after the start of the next semester. These mailing lists/groups can be generated according to the course numbers, for example, CS555@iiitd.ac.in.

Managing lists/groups in IIIT-D domain

- When lists/groups are available?
  - Course lists/groups are available one week before start of classes.
- Use of lists/groups
  - Student mailing lists should be available only to Director, Dean Academic Affairs, AM Academic Affairs, Chair - Seminar Organizing Committee, Chair and AM - IT Resources Committee, student representatives, Heads of the Centres and Google Apps administrators. If anyone else needs to send any important email to the students, they can send their request to the respective above-mentioned person, depending upon the objective of sending the email.
  - The staff Manager is the owner of the office mailing list and it is available for posting to the list members and the Director
  - The Director is the owner of the faculty mailing list and it is available for the posting to all the members
  - Instructor is owner of course mailing list and by default the instructor can post to the mailing list.
  - The faculty members of the research groups are owner of the respective research groups' mailing lists/groups and they can decide policy about posting
- What are methods add or delete members in the list?

    - Owner of the list can do this or IT Dept. can also do the same on request from group owner.
    - In a complaint case, Google Apps administrator or IT Department with prior approval from Chair IT committee can add or delete any particular user from any emailing list by informing group owner only.
    - Director can ask for addition and deletion of any group member for any permission to any group or for the entire group itself. In case of such change, the owner of the group will be informed.
- What are methods for requesting use of lists for some purpose?
    - If anyone wants to send an email to a mailing list, the person should send a request to the mailing list's owner, who then decides and takes the action accordingly.

Internet usage and privacy
This policy will apply.

email monitoring and access log view
Google Apps does not provide passwords of individual accounts to Google App admins. Individual account can be accessed by resetting password of that acount. Google Apps maintains a log containg logins times and who sent emails to whom. The IT Department may monitor or view the email logs and access individual accounts in case of following circumstances:

- Excessive utilization of email has been detected.
- There is a security breach, which needs to be traced and analyzed.
- Malicious traffic from some IDs has been detected.
- There is a complaint from Law Enforcement Agencies.

In the scenarios 1-3 above, email logs or individual account from Google Apps can be viewed as and when required by IT Department after approval of the IT committee to identify the source or cause of the issue. In scenario 4, email logs or individual account from Google Apps can be viewed by IT Department only on prior approval from Director and IT committee.

Access to email logs and individual account will be available only to Google App admins and will be protected through best practices for email security.

Conducting experiments on IT-resources of the institute

- Any experiment or survey should not
    - Collect of confidential information, e.g., passwords, credit card number, PAN number, etc
    - Hamper smooth functioning of the IT system, e.g., jamming of WiFi, creating rogue WiFi APs, stealing IP addresses, etc.
- Individual email IDs or lists/aliases/groups

    - The student must get an approval from the concerned owner of the email ID and the faculty, who is directing the experiment
    - The student must get an approval from the concerned owner of the lists/aliases/groups and the faculty, who is directing the experiment
- Lab PCs
    - Use of lab PCs for experiments is discouraged. Server is a better option. In case a server is unavailable, the student must get an approval from the concerned faculty and the IT Committee Chair
    - The student and the concerned faculty must get an approval of the owner of the server
- Firewall data
    - Permission of IT Committee is required
- Network
    - To get access to registered MAC addresses of devices connected to the campus network, permission of IT Committee Chair/Director is required
    - To install any device, that modifies packets, on the wired ethernet, an approval from the IT Committee Chair/the Director is required
    - To install a WiFi Access Point, an approval from the IT Committee Chair/Director is required
    - To use an external IP, faculty will get an approval from the IT Committee Chair/Director
- Web server to host web applications
    - The student must get an approval from the concerned faculty and the IT Committee Chair
        - If the server is in iiitd.ac.in domain, approval of the Web Coordinator is also required
    - The Director can request to hold any web application

Managing of IT-resources of the institute

- Damage and loss of equipments
    - JM (SA&N) requests AM (Students Affair) to maintain a log of all the damages, whose costs may be recovered by the institute from students

Managing Backpack/Moodle

- Checking log
    - The faculty can request access to log of his/her course to backpack Admin
    - The Director can requests access to log of any course to backpack Admin

Managing file server

- Checking files in the file server
    - Institute has Network unified storage though which file server facility being

given. Presently file server space has been allocated to faculty, staff, and PhD students. Any other users may request for file server space by taking necessary approval from concerned faculty or department manager.

HPC usage guidelines

Please refer attached link for HPC Guidelines