Privacy Policy for IT usage at IIT Delhi

Keeping in mind the internal security requirement of IITD, applicable Law and to ensure as far as possible full privacy for all legitimate use if IITD IT facilities to all students, staff, faculty and visitors the **Deans Committee** in its meeting on December 16, 2016, has decided on the following **Privacy Policy**.

Use of encrypted channels and digital certificates

1. All facilities in IITD that require users to provide their passwords are set up over encrypted channels (https/SSL/TLS/kerberos) using strong 1024/2048 bit encryption.
2. All encryption facilities are signed using either a valid external Certficate or the IITD CA certificate issued by the CSC (see certificates) which the users are advised to verify before providing their passwords.

Privacy of User data & Meta-data

1. As a general rule CSC will respect users privacy regarding their data and meta-data. No CSC administrator will directly access user data such as mail, homes, or other stored content. Automated tools may process some of this for backup, deduplication and other routine functions as well as relevant statistics and usage collection. In addition automated malware/antispam tools may access the data to flag any illegal/malicious content and or mine the metadata to build relevant usage details.
2. The administrators follow a policy of never accessing the content of any mailbox or user data or access details, unless required (or instructed) to do so as a part of an investigation of any misdemeanor. Certain automated scripts/programs may report IT usage violations which may require investigation. Also in case of a formal complaint either internal, or received externally from law enforcement agencies, the access logs/email records other user data may be examined by authorized CSC personnel only to investigate the complaint. Please note that in the case of an a complaint or , Such investigations typically require the consent of the IT Discipline Committee or the Director or his nominee.

Email privacy

1. All users including faculty, staff and students are provided an official email id in the domain iitd.ac.in. According to IITD policy all users are expected to use this email id in all official correspondence.
2. Mail exchange with all clients is carried out over a secure encrypted channel.
3. Mail exchanges with other servers outside IITD are carried out using opportunistic TLS encryption. The exchange is encrypted if the other server supports it, and is over a plain text channel otherwise. Decryption keys for all encrypted transfers will be provided to designated law enforcement agencies only if such requests are in accordance with the IT Act of the Government of India.
4. The email system is set up using a set of mailstore, smtp and imap servers. None but the administrators have login access to these servers and access to the mailboxes are provided through imaps (over encrypted TLS/SSL channels) protocols. Designated system administrators have root access on this server and can access all mailboxes. The administrators follow a policy of never accessing the content of any mailbox as root, unless required (or instructed) to do so as a part of an investigation of any misdemeanor (see Privacy of user data & Metadata bullet 2 above).
5. Logs of all email transactions (both in-bound and out-bound) are maintained for 26 weeks after which they are automatically deleted. Again, the administrators have access to these logs. Automated programs may be run by administrators to generate performance statistics and/or to train tools for spam and misuse detection. The administrators follow the policy of never examining the contents of the log to determine who sent mails to whom unless they are required to do so as a part of investigation of misdemeanor, or for debugging mail problems.
6. The mail server is configured to accept incoming mails for only valid user in IITD. The mail server does not relay any mails without authentication.
7. The smtp server is configured not to accept mails from servers which are on the banned RBL list or are known open relays.
8. The web-mailer available through the IITD web-page is available to all users for accessing and sending. All transactions (not merely authentication) are carried out using the secure https protocol (over SSL).
9. All mails delivered through the IIT Delhi servers are digitally signed, and the receiver of the email can cross check the authencity of the mails originating from IIT Delhi (see Digital Signing of emails).
10. The authenticity of any email that is accepted cannot be guaranteed by the mail transfer protocol. All users are advised to cross check in case of doubt or use digitally signed emails. In case emails are digitally signed, the authenticity is certified by the certificate provider and it is the user's responsibility to verify the certificates.
11. All mails from our administrators will be signed by a self-signed or external certificate..

Web server privacy

1.

Users who are provided with facility to create their own web-pages, both for world-wide access (of the contents of the public_html directory) and restricted access from within IITD (of the contents of their private_html directory, are solely responsible for the contents of those web-pages.

2. The web accesses are logged for 26 weeks after which they are automatically deleted. The logs may be mined to generate access and performance statistics. The logs are accessible to the administrators who normally never examine them manually unless required to do so for the purposes of investigation of misdemeanor or debugging.

Proxy-server privacy

1. All users may access the web through the IITD proxy server, where they are required to provide their passwords. The passwords are never logged.
2. Access of pornographic and some other offensive web-sites are blocked by the proxy-server. The access control list is downloaded periodically from standard sites (RBL) which maintain upgraded lists of sites providing offensive contents. However, these mechanisms are not entirely fool-proof.
3. The accessed pages are cached unless there are explicit `direct' directives (in http protocol) from the web servers. All mail hosts like hotmail, yahoo and gmail are expected to use such directives for email content, which consequently is never cached. The cached pages are neither mined nor examined. However, such examinations may be carried out for investigation of misdemeanour.
4. Web access records of all users are logged for 26 weeks after which they are automatically deleted. Mining of the logs may be carried out automatically to generate performance and usage statistics. Also, the data may be mined automatically to determine the top down-loaders of the day. If such downloads are perceived to be unreasonable (by the administrators) then an explanation may be sought from the user. The policy of manual examination of the logs by the administrators is similar to that of the mail logs described above.

5. Please note that in the case of a complaint (see Privacy of user data & Metadata bullet 2 above) the access logs may be examined by authorized CSC personnel to investigate the complaint. In case the IT Discipline Committee and institute authorities deem necessary as per

applicable law, the impugned access details may be provided to the concerned external agencies.

Privacy of home directories and Owncloud

1. All users are provided a home directory in the CSC. The quotas are set according to user groups. In addition all users have access to the CSC owncloud storage.
2. The home directories and owncloud files are maintained on the NAS file server and are made available to all (trusted) machines in the cluster via NFS and/or CIFS protocols.
3. The users are responsible for setting the access permissions of their files as per standard Unix conventions.
4. Irrespective of the permissions the administrators can access all user files. They shall not do so unless explicitly requested by a user/owner. They however may be required to do so for investigation of misdemeanors, the conditions for which are similar to those mentioned above. They may also change file permissions in such cases. This will usually require the consent of the the Director or his nominee.
5. Home directory over NFS/ CIFS of a user will be provided strictly over Kerberos authentication.
6. Owncloud files can also be accessed from outside IIT Delhi and can be shared with others via links as per their owncloud settings. Users should take appropriate care when sharing.

Privacy of passwords

1. The passwords are maintained on the Kerberos server in encrypted format and are never logged.
2. The administrators may run standard password crack softwares on the encrypted passwords during routine security audits. Users are advised if their passwords are found to be weak.
3. The CSC will normally never request the users for their passwords, and the users are expected to protect their passwords against any form of phishing. In case the CSC requires the users to register their passwords for some facility, such request will be made through duly

authenticated or hard copy notices signed by appropriate authority.

Security

No Quality of Service guarantees for security can be given. However, the following routine precautions are adopted.

1. Only administrators are authorized to login to the mail, web, proxy and other servers.
2. Security advisories on the software currently being used (OS components, sendmail, squid proxy, apache etc) are regularly monitored. At least one designated system administrator receives an email alert whenever such an advice is released by the official maintainers of the software. The software is updated periodically and whenever required.
3. All ports except those necessary for functioning of the servers are blocked (firewalled) both from outside and inside.
4. Standard intrusion detection software is run on the LAN to monitor any change of MAC addresses corresponding to IP addresses of trusted machines. A designated administrator automatically receives an email alert in such cases.
5. Kerberos is used for authentication across the systems in CSC. The administrators carry out routine checks to spot unusual access patterns on a `best effort' basis.