CUTS IT POLICY

Contents

1. Introduction

1.1 Information Security

Information security policies are the cornerstone of information security effectiveness. The security policy is intended to define what is expected from an organisation with respect to security of information systems. The overall objective is to control or guide human behaviour in an attempt to reduce the risk to information assets by accidental or deliberate actions.

Information security policies underpin the security and well-being of information resources and are the foundation and bottom line of information security within an organisation.

Data security will help the user to control and secure information from inadvertent or malicious changes and deletions or unauthorised disclosure. There are three aspects of data security:

Confidentiality: Protecting information from unauthorised disclosure like to the press, or through improper disposal techniques, or those who are not entitled to have the same.

Integrity: Protecting information from unauthorised modification, and ensuring that information, such as a beneficiary list, can be relied upon and is accurate and complete.

Availability: Ensuring information is available when it is required. Data can be held in many different areas, some of these are:

- Network Servers
- Personal Computers and Workstations
- Laptop and Handheld PCs
- Removable Storage Media (DVD/CD-ROMs, External Hard Disks, Flash Drives etc.)
- Data Backup Media (External Hard Disks and Network Access Storage Devices)

1.2 Data Loss Prevention

Leading Causes of Data Loss:

- Natural Disasters
- Viruses
- Human Errors
- Software Malfunction
- Hardware & System Malfunction

Computers are more relied upon now than ever, or more to the point the data that is contained on them. In nearly every instant the system itself can be easily repaired or replaced, but the data once lost may not be retraceable. That's why of regular system back-ups and the implementation of some preventative measures are always stressed upon.

1.3 Natural Disasters

While the least likely cause of data loss, a natural disaster can have a devastating effect on the physical drive. In instances of severe housing damage, such as scored platters from fire, water emulsion due to flood, or broken or crushed platters, the drive may become unrecoverable.

The best way to prevent data loss from a natural disaster is an **off-site back up**. Since it is nearly impossible to predict the arrival of such an event, there should be more than one copy of the system back up kept, one onsite and one off.

1.4 Viruses

Viral infection increases at rate of nearly 200-300 new Trojans, exploits and viruses every month. There are approximately 65135 '*wild*' or risk posing viruses. With those numbers growing every day, systems are at an ever-increasing risk to become infected with a virus. There are several ways to protect against a viral threat:

- Install a Firewall on system to prevent hacker's access to user's data
- Install an anti-virus program on the system and use it regularly for scanning and remove the virus if the system has been infected. Many viruses will lie dormant or perform many minor alterations that can cumulatively disrupt system works. Be sure to check for updates for anti-virus programme on a regular basis.
- Back up and be sure to test back-ups from infection as well. There is no use to restore virus infected back up.
- Beware of any email containing an attachment. If it comes from anonymous sender or don't know from where it has come or what it is, then don't open it, just delete it & block the sender for future mail.

1.5 Human Errors

Even in today's era of highly trained, certified, and computer literate staffing there is always room for the timelessness of accidents. There are few things that might be followed:

- Be aware. It sounds simple enough to say, but not so easy to perform. When transferring data, be sure it is going to the destination. If asked '*Would you like to replace the existing file*' make sure, before clicking "yes".
- In case of uncertainty about a task, make sure there is a copy of the data to restore from.
- Take extra care when using any software that may manipulate drives data storage, such as: partition mergers, format changes, or even disk checkers.
- Before upgrading to a new Operating System, take back up of most important files or directories in case there is a problem during the installation.
- Never shut the system down while programmes are running. The open files will, more likely, become truncated and non-functional.

1.6 Software Malfunction

Software malfunction is a necessary evil when using a computer. There are still few things that can lessen the risks:

- Be sure the software used is meant ONLY for its intended purpose. Misusing a programme may cause it to malfunction.
- Using pirated copies of a program may cause the software to malfunction, resulting in a corruption of data files.
- Be sure that the proper amount of memory installed while running multiple programmes simultaneously. If a programme shuts down or hangs up, data might be lost or corrupt.

1.7 Hardware Malfunction

The most common cause of data loss, hardware malfunction or hard drive failure, is another necessary evil inherent to computing. There is usually no warning that hard drive will fail, but some steps can be taken to minimise the need for data recovery from a hard drive failure:

- Do not stack drives on top of each other-leave space for ventilation. An over-heated drive is likely to fail. Be sure to keep the computer away from heat sources and make sure it is well ventilated.
- Use an UPS (Uninterruptible Power Supply) to lessen malfunction caused by power surges.
- NEVER open the casing on a hard drive. Even the smallest grain of dust settling on the platters in the interior of the drive can cause it to fail.
- If system runs the scan disk on every reboot, it shows that system is carrying high risk for future data loss. Back it up while it is still running and ensure that the NAS incremental back up is up and running.
- If system makes any irregular noises such as clicking or ticking coming from the drive. Shut the system down and call IT for more information.

2. Procurement Policy

2.1 Purpose

2.1.1 The organisation routinely seeks goods and services from the market from various suppliers and contractors in pursuance of its work areas. It is considered expedient to lay down rules, principles and procedures to facilitate such procurement leading to cost effective and competitive rates along with transparency and accountability.

2.1.2 The following general principles and procedures shall be observed in carrying out procurement of goods and services by all CUTS Centres with the only exceptions as to other agreements CUTS may otherwise come into terms with.

2.1.2.1 General principles

The following principles would be adhered to:

- ✓ *Competitiveness*: The procurement must be made on the basis of adequate search for the most qualified suppliers/contractors.
- ✓ *Transparency*: The procurement process would be transparent and with the participation of several individuals concerned in the decision-making process.
- ✓ *Accountability*: An appropriate record and information, oral or written, in respect of procurement shall be maintained.

2.1.2.2 Steps in procurement process

- ✓ All fixed assets would be approved for purchase by the head office (HO). However, other procurements such as those related to consumables, maintenance contracts, repairs of assets, organizing events, etc. up to Rs10,000/- per reference would be permissible at centres.
- ✓ Procurement for services pertaining to organizing events under projects would be requisitioned by outstation centres in their request for monthly funds. Centres in Jaipur would use Annexure 1 as also the advance requisition form already in use.
- ✓ Request for procurement would be received at the Finance and Administration (F&A) division at HO on the format at Annexure 1 duly filled in and forwarded to HO by the Centre head. This would contain justification for purchase of services and details of budget available, if any, under projects which are being implemented.

- ✓ F&A would verify details submitted by the centres and assess required outputs, its quality, time-frame, required suppliers/contractors, financial implications, etc. and prepare a note on Annexure 2 for the sanctioning authority, which is as under (per reference)

Up to Rs10,000	- Centre Head/Assistant Director (F&A)
Between Rs10001 and Rs5,00,000	- Dy. Executive Director
Between Rs5,00,001 and Rs25,00,000	- Secretary General
Above Rs25,00,000	- Executive Committee

- ✓ The basis of annexure 2 would be the request for procurement and at least three independent quotations procured from relevant suppliers/contractors and a summary of the department's assessment vis-à-vis price, availability of guarantee, local servicing, training if required, delivery schedule, terms of payment including penalty for sub-standard or delayed supply, technical requirements wherever needed, status of supplier, reports of the supplier (from client list).

- ✓ Upon approval, issue a purchase order in writing and verify services either themselves or through the concerned programme staff and centre head and make payment on agreed terms.

2.1.2.3 Exceptions

- ✓ In emergent circumstances, the requirement for quotations may be waived. Such cases, regardless of the value of the procurement, must be reviewed by a Panel comprising the Secretary General, the Executive Director and the Deputy Executive Director. In permanent or temporary non availability of one of them, one of the Directors of CUTS would be a part of the panel.

- ✓ Settling of the amounts payable to the partners or individuals in execution of projects would remain outside the purview of this policy unless specified by the donor. In such cases, the project team would jointly arrive at amounts payable and inform the F&A department.

- ✓ Prices or rates fixed pursuant to national legislation or by regulatory bodies, standardization of supplies, equipment or spare parts that render competition impracticable, purchases that cannot be delayed and a previous order or contract awarded to the lowest bidder and it is advantageous to award an order for a new identical requirement to the same bidder at the same price would also fall in the category of exemptions.

4. Audit Policy

CUTS conduct bi-yearly interim audit of IT assets by updating the list online. The scanned copy of the same is duly verified and signed by the Centre Head and the person conducting the audit and maintaining the inventory of the respective Centre which is sent to HO. The deadline is fixed for the same.

An additional Google calendar reminder for the aforesaid process is also sent to help accomplish the task in a streamlined manner. There are two sets of reminders, one is a monthly reminder which will remind all about updating the inventory file and take back up, and the second set is for the half yearly and annual inventory report that is to be sent across to the IT team in Jaipur.

5. Asset Issuance Policy

As a part of efforts to streamline process and ensure statutory audit compliance it is necessary to maintain a record of IT assets.

An issuance sheet is a record of movable IT equipment issued to staff of the organisation. This equipment is issued either on a long- or short-term basis and once it is being issued, it is imperative for us to keep a record. In the case of long-term issuance only a declaration/undertaking form needs to be signed whereas in the case of short-term issuance an issuance sheet needs to be signed in adherence to the terms and conditions specified/stated in the declaration/undertaking form.

It is important to do so to ensure that there is proper accountability of assets once they are issued to somebody especially in the case of loss, theft or damage. In order to ensure that we are in complete compliance with statutory audit requirements we have streamlined the process which will now include

1. **Issuance Sheet:** This will have to be signed for short term issuance by the user at the time of receiving the asset and by IT team when the asset is returned

2. **Declaration/Undertaking Form**: To be signed for long term issuance by the user to acknowledge that the person has received the article in the condition as specified in the form and that the same will be returned by the user in the same condition to the IT department. And once issued the user will be responsible for its maintenance and upkeep. In case of loss, theft or damage the user will have to reimburse the organisation to the tune of the financial value of the asset on the said date.

IT will continue to provide the support services for hardware and software however for loss, theft, damage etc. the liability lies with an individual. Hence, as a part of the compliance requirement, the IT department will be getting the form signed by the concerned users for proper record keeping.

6. Policy for General Users

Using CD/Flash Drives

- CDs or Flash Drives should be used with utmost care after scanning and ensuring that the .exe files in it are safe to run from IT in-charge.

Password

- Share official workstation password with IT.
- User should not have easily detectable passwords for Network/Email access etc.
- A strong password must be as long as possible, include mixed-case letters, include digits and punctuation marks, not be based on any personal information, not be based on any dictionary word, in any language.
- Never use the same password twice.
- Change password at regular intervals.

Backup

- Backup should be maintained regularly on the space (folder with user initials) provided on workstation as per IT guidelines.
- Ensure that data backup is running on workstation.
- Keep any personal or sensitive data out of the official folder specified to backup the data on to Network Attached Storage (NAS).

Physical Safety of System

- Protect the system from unauthorised use, loss or damage.
- Keep portable equipment's like external HDD, Flash drives etc. secure.
- Seek advice on disposal of equipment
- Report any loss of data or accessories to the System Administrator/in-charge IT
- Keep the system and sensitive data secure from outsiders
- Get authorisation before taking equipment off-site
- Take care when moving equipment (Read instruction on moving equipment)
- Install UPS system with adequate battery backups to avoid any data loss or corruption due to power failure
- System should be properly shut down before leaving the office
- Log-off the system if you are leaving your seat
- Never remove the cables when your PC is powered ON since this can cause an electrical short circuit
- Do not stop scandisk if system prompts to run it at the time of system startup
- Always use mouse on mouse pad
- Be gentle while handling keyboard and mouse
- Do not open case of the hardware
- Make sure that there is some slack in the cables attached to your system

Computer Files

- Then user permission for individual files, folders, drives should be set.
- Any default shares should be removed.
- Only required file and object shares should be enabled on the server/client.
- Never download or run attached files from unknown email ID.
- Always keep files in the computer in organised manner for easy accessibility. Keep all the official files in the specified folder on the workstation with user initials which is synchronized with NAS for real-time data backup and disaster recovery.
- Avoid creating junk files and folders.
- System files and libraries should not be accessed as it can cause malfunctioning of system.
- When transferring data, be sure it is going to the destination. If asked '*Would you like to replace the existing file*' make sure, before clicking 'yes'.

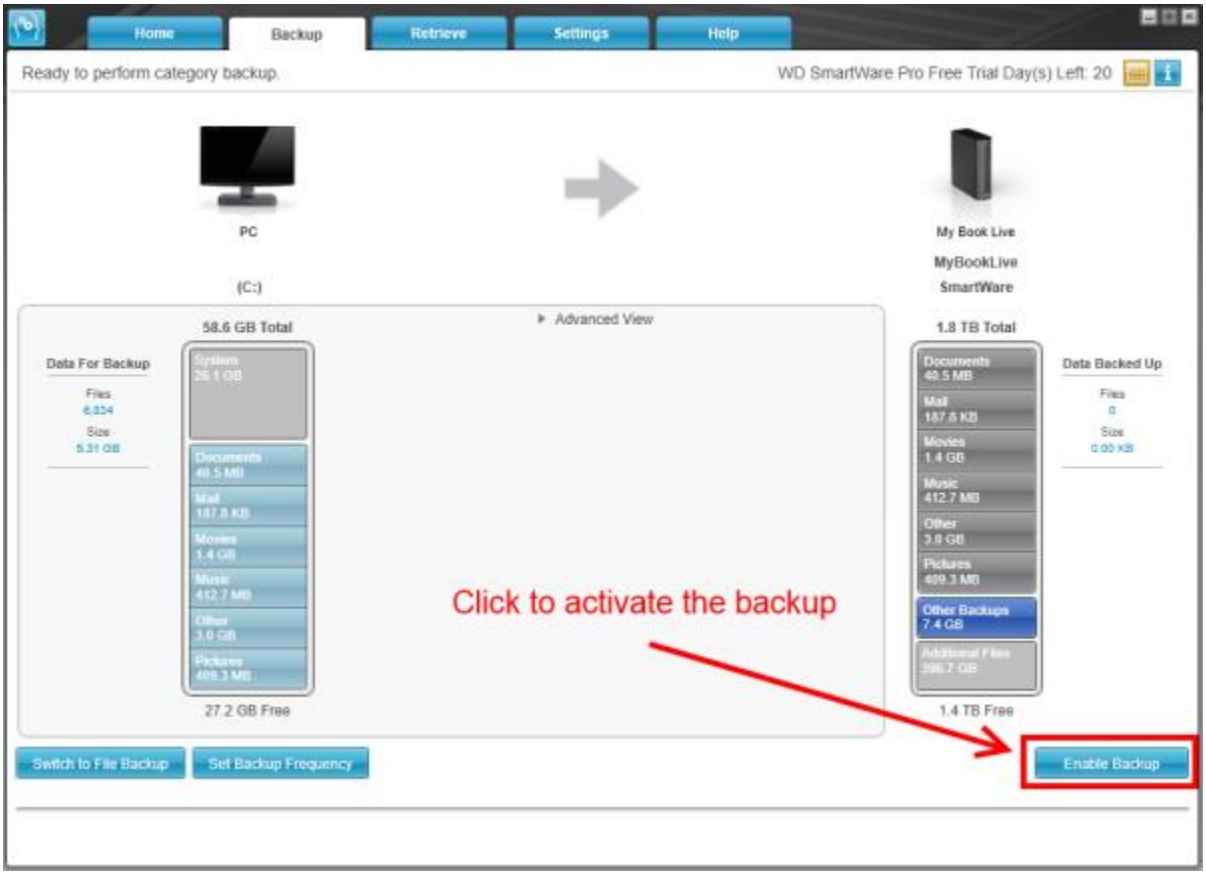
General Instructions

- In case of uncertainty about a task, make sure there is a copy of the data to restore from backup device like Network Attached Storage (NAS)
- Follow instructions or procedures that comes from System administrator/Incharge computer centre time to time
- Users are not supposed to do his or her personal work on computers
- Please intimate System administrator/Incharge computer centre in case of system malfunction.
- User should always work on his/her allotted machines. In case of any urgency/emergency user may use other's machine with consultation of System administrator/Incharge computer centre
- Antivirus software should be updated timely in consultation with System Administrator/Incharge computer centre
- Do not use unnecessary shareware.
- Do not install or copy software on system without permission of System administrator/Incharge computer centre
- Avoid unnecessary connectivity of Internet
- Don't panic in case system hangs. Report it your IT Nodal Officer/System Administrator/Incharge computer centre
- Please ensure that preinstalled Antivirus is running on the system
- Food and drinks should not be placed near systems. Cup of Tea/ Coffee or water glass should not be on CPU or Monitor or Key Board.
- Always power off the system when cleaning it.
- Never use wet cloth for wiping the screen.
- Never shut the system down while programs are running. The open files will, more likely, become truncated and non-functional.

7. SoP for Security Devices and Admin Panels

Network Attached Storage

The WD Smartware NAS software supports automatic backup of the computer drives, My Documents, Desktop, and Favorites to NAS. When source files are added, modified or deleted, the changes will be synchronised with the destination automatically. Users should store all the official data into the specified folder with user initials which is synchronized with WD NAS on an incremental basis which means after the first time data backup, WD Software only copies the changed files since the last backup.



SOPHOS Unified Threat Management

In order to provide seamless IT services to all, CUTS is having a secure, reliable and centrally managed network and firewall in the office. It has been programmed to block potentially obtrusive and harmful website such as Torrents, Porn sites, Malware, Adware etc. These safeguards have already been deployed on our system and it has been ensured that all work related sites remain available to users. Time to time firmware and version updates are done to keep the device equipped with latest patches to fight new threats.

8. Setting Default Language and Style

CUTS is having its Style Guide which aims to provide a guide to writing and formatting documents written by staff on behalf of the organisation with the primary objective of ensuring that the organisation's formal documentation is presented consistently across all forms of communication. This style guide sets up CUTS' preferred spellings and terminology, along with general guidance on English Grammar, style and usage.

Font

Setting default font and font size in MS Word

- Open blank document
- In the Font group, click the Font fly out
- Select the options that you want to apply to the default font, such as font style and size
- Click Set As Default
- Select All documents based on the Normal.dotm template? option, and then click OK

Setting default font and font size in Gmail

- Click on the General tab of the settings and find Default text style
- Adjust the font-face, size, style, and colour of the text of your choice

Language

Setting default language in MS Word

- Click on the **Review** tab
- Under **Language**, click on **Set Proofing Language**
- A window will appear on the screen labelled **Language**. Highlight your preferred language by clicking on it
- Click **Set as Default** and **OK**

Setting default language in Gmail

- Right-click in the text field and change the dictionary from the Languages entry on the menu

- Uncheck Use this language for spell checking from other languages and check the option for the desired one

Signature Line

There is a fixed template for e-mail signature lines. Sans Serif small size grey colour font with right alignment is used. It has been communicated to all users to keep the template of signature line in the prescribed format only and not to amend/temper at all.

9. Smartphone Policy

CUTS is giving internet and intranet facility on the handheld/mobile devices of the senior managers. They are MAC address bounded with the UTM device with bandwidth control of up to 1 Mbps and firewall rule of intrusion protection. If any guest or intern arrives at CUTS then by the specific request of HR department and the concerned a guest ID to access internet is provided to them for a specified time period which expires automatically after the exhaustion. The time period can be further altered as per the requirement and the request of HR department and the concerned.

10. Email Policy

Using your web-based email account

- Go to the URL: http://mail.google.com
- Feed your email ID as your username i.e., xyz@abc.com and password
- Account holder will be then redirected to the "CUTS Gmail Server" portal which carries email account of the user

Few Useful Gmail Features

- **Spam filtering**: Spam is another name for junk email. Gmail uses advanced technologies to keep spam out of your inbox. Most spam is automatically sent to a separate spam folder, and after 30 days it is deleted.
- **Conversation View**: An email conversation occurs whenever you send emails back and forth with another person (or a group of people), often about a specific topic or event.
- **Labels:** Allows you to organize your messages and make them easier to find. Applying a label to a message is kind of like putting it into a folder, with one important difference: You can apply more than one label to a message.
- **Attachment Reminder:** While composing any new mail if you have written a phrase like "I have attached files "and hit send without actually attaching any files. Google will recognize it and will pop up a message saying "It seems like you forgot to attach, you wrote "I have attached "in your message but there are no files attached .send anyway?". That way Google can save you from any kind of embarrassment.
- **Add Multiple Accounts in Gmail:** Gmail provides multiple sign-in facility to switch between different Gmail accounts in same browser without having to sign out and back in again. To add account simply click on profile picture in top right corner then you will get "ADD ACCOUNT' option Click on it, it will open sign page in new tab.
- Undo Send: If you accidentally sent a message, want to undo it enable Undo Send. It will stop messages from being sent for a few seconds after hitting the send button.
- **Gmail Offline:** It helps you to access mails and compose new mails while you don't have internet connection or unreliable connections or slow. When users reconnect, Gmail automatically sends any outbound messages. Maximum synchronization period for data is 30 days.

- **Google Hangouts**: It is a unified communications service that allows members to initiate and participate in text, voice or video chats, either one-on-one or in a group.

We have created new email groups so that if an individual member of staff wants to address a complete department/office they can do so by simply typing their group email address rather than keying in names of all the members of that particular team. The following groups have been created for our usage. The names given to the groups are self-explanatory.

Sl No	Group Name	Group Email address
1	All Staff	allstaff@cuts.org
2	All Accra	allaccra@cuts.org
3	All Lusaka	alllusaka@cuts.org
4	All CART	allcart@cuts.org
5	All CCIER	allccier@cuts.org
6	All Chittorgarh	allchittorgarh@cuts.org
7	All CITEE	allcitee@cuts.org
8	All Kolkatta	allkolkatta@cuts.org
9	All Delhi	alldelhi@cuts.org
10	All Finance	allfinance@cuts.org
11	All Geneva	allgeneva@cuts.org
12	All HO	allho@cuts.org
13	All HRAdmin	allhradmin@cuts.org
14	All Hanoi	allhanoi@cuts.org
15	All India	allindia@cuts.org
16	All IT	allit@cuts.org
17	All Jaipur	alljaipur@cuts.org
18	All Nairobi	allnairobi@cuts.org
19	All Publications	allpublications@cuts.org

For example, in Jaipur, we have three offices located in three different places and if we wanted to send information only to the Jaipur staff we were having to key in the names manually one by one. Now we can simply send the emails to all of them by typing in alljaipur@cuts.org and the email will go to all staff based in Jaipur. Similarly, if you need to take leave and have to inform HR in addition to your line manager, you can simply mark the email to you line manager and include allhradmin@cuts.org in CC and the mail will come to all of us in HR.

All of you are encouraged to use save these groups in your address books and start using them in order to reduce the time taken to compile emails. Please do exercise caution while selecting and including a group in an email. Use group emails only for general notifications which are meant for all the staff of a unit. If you need to include a person outside the unit then please include their email ID separately.

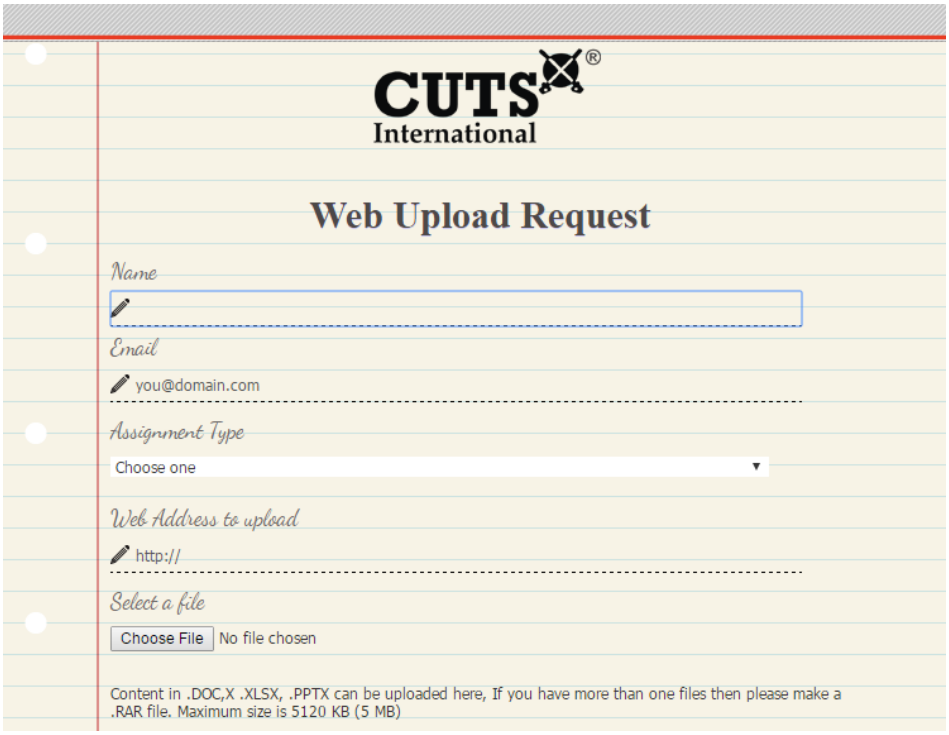
11. Web Policy

Till date, web upload requests were sent by email and did not clearly indicate where the document was to be uploaded on the site. This led to delays due to the time spent in ascertaining the location of the document and also created multiple reference points for the IT team from which to ascertain their task list.

Considering the above, a proper mechanism has been put in place and a Web Upload Request Form has been devised. The new form will help streamline this process for everyone and will put the onus of defining the upload location on the sender rather than on the IT team.

This will not only ensure timely uploading in a streamlined manner but will also increases accountability of colleagues sending requests for web upload and of the IT department since all requests will now be stored in one place and can easily be monitored for progress.

This is the form: http://goo.gl/8IqhnW



Users should create a book mark of the form on their browser so that it can be accessed readily. Any requests for web upload that are not sent through this form will not be accepted and entertained.

References

1. https://www.csoonline.com/

2. http://www.nsit.ac.in/
3. http://www.customguide.com/