



IT and Data Protection Policy

Created: August 2010

Recent Update: September 2015

Contact Information: 17/18, N block, Gulberg II, Lahore – PAKISTAN.

Telephone: 042-35779030-1

Website: www.bargad.org.pk

Table of Contents

Table of Contents	1
Organizational Profile	2
1. Purpose	3
2. Policy	3
3. Standard Operating Procedures (SOPs):	3
3.1 Limited permission for personal use of BARGAD computer/related equipment's	3
3.2 BARGAD Right to Access	3
3.3 Restrictions to Access	4
3.4 Use of the internet	4
3.5 Use of Email	4
3.6 Responsibilities of Employees	5
3.7 Maintenance of Computer Systems	5
3.8 Disaster Recovery Plan	5
3.9 Security of Data	6
3.10 Security of Server Machines	6
3.11 Database/Software credential and backup	7
3.12 IT- Person Substitution	7
3.13 Administrative Guidelines	7
3.14 General Guidelines	7

Organizational Profile

Bargad is a youth development organization actively working to promote peace, justice and cooperation amongst the youth¹ in Pakistan. The organization has focused on creating opportunities and amplifying the voices of the youth ever since its inception in 1997, leading to a vast network of around 3000 youth volunteers, known as the Bargad Volunteer Network (BVN) throughout the country.

Bargad's Vision:

Politically, socially and economically empowered youth and women, respect, protect and promote peace and harmony

Bargad's Mission:

1. Engage vulnerable youth and women in all diversity to their full potential through education, mentorship and innovative interventions designed to enhance their overall well-being.
2. To invest in youth-led and youth-centred ideas, to convene key stakeholders in the sector and advocate for systems and policy changes that meet youths' needs.
3. Engage youth to end violence against women.

Bargad has implemented more than 100 projects on youth training², youth mobilization and policy advocacy, including the provision of technical assistance to all the provincial governments of Pakistan, regions of Gilgit-Baltistan and the State of Azad Jammu Kashmir (AJK) for the formulation of their respective youth policies. These policies have been approved by the provincial governments of Punjab (2012), Khyber Pakhtunkhwa (2016) and Sindh (2018), resulting in governments' pledges to allocate 4% budget to sports and youth affairs, 15% on the women employment quota, implementation of the E-Rozgar programs, and on youth participation in the local governments, respectively. Bargad has also conducted Capacity Enhancement workshops on youth development with officials of the youth affairs departments of Punjab, Balochistan and Sindh.

Bargad has a youth network of 782 individuals, civil society organizations and government institutions, with Youth engagements with 64 Universities, 40 Colleges and 35 Higher Secondary Schools.

The organization has previously partnered with 26 membership-based student organizations and 15 Youth Groups over Pakistan; producing the largest pool of researches and publications on various aspects of youth than any other civil society organization in Pakistan, while also pioneering a youth track of peace and diplomacy in the South Asian region.

The hallmark of the organization is that its core youth volunteers participate in all aspects of the projects - from action-planning to project execution, while also mapping in the course of its work; issues as well as challenges identified by the youth across the country³.

¹ Adolescents: 12-19; Youth age bracket in Pakistan: 15-29

² Since 2003, the organization has trained 7880 youth activists and young faculty only through training workshops and peer sessions in issues of social development.

³ The Youth in the mapping is part of the Youth Cohorts in the districts where Bargad has actively worked or is presently working.

1. Purpose

To maximise the productivity of all BARGAD employees, they are encouraged to use the electronic media available such as the Internet, e-mail and intranet to their optimum potential. This policy will stipulate the guidelines for the access and use of the IT related resources.

Employees should read and abide by these Guidelines. Additional policies as decided by the management from time to time may apply to specific computer systems or networks provided.

2. Policy

- a. All electronic media systems including e-mail, the Internet, hardware, software, local area network, files, and all information composed, transmitted, accessed, received or stored in these systems are the property of BARGAD.
- b. The systems are to be used for conducting BARGAD 's business only and the use of this equipment for personal or unofficial purposes or for personal financial or other gain are strictly prohibited unless it is specifically approved by the management.
- c. All employees need to ensure that computer access passwords provided to them are kept confidential with them at all times.
- d. Each employee is responsible for the security and safe custody of information stored on his/her computer.
- e. All data regarding the research, information of participants, children / vulnerable adults should be kept confidential till the approval from the Bargad management.
- f. Breach of confidentiality access can result in losing access to network and/ or disciplinary action.

3. Standard Operating Procedures (SOPs):

3.1 Limited permission for personal use of BARGAD computer/related equipment's

The workstations/computers will be used by authorized personnel and for official purposes only. These assets will not be issued for the personal use. In case the assets are required to be issued for the purpose of office work outside the premises, the issue will be approved by the competent authority on written request. The staff will be responsible of returning the equipment in good order and will be responsible for any intentional loss/damage to the equipment.

3.2 BARGAD Right to Access

BARGAD may exercise its right to review, audit, intercept, access and disclose all matters on its systems at any time, with or without employee notice, during or after working hours. Employees should have no expectation of privacy in connection with the use of these systems.

3.3 Restrictions to Access

BARGAD reserves the right to block access to certain Internet web sites and other resources, which pose a security concern or are otherwise, not related to BARGAD's activities and objectives.

3.4 Use of the internet

Although, the users are allowed to use the internet on a limited scale, however, they are expected not to download un-authorized games/software/video clips etc. so that the bandwidth is not choked and regular office work is not affected.

IT Officer, with the authority of management, may monitor Internet accesses for the purpose of optimising network utilization.

BARGAD will not monitor the content of electronic mail or of other Internet transmissions unless a complaint is received or there is reason to believe that a violation of security or of BARGAD Policy has occurred. However, URLs of all web requests, envelope data of electronic mail, and similar details of other connections may be logged.

Only authorised user may have internet access. This authorisation may be re-assessed by the management from time to time.

3.5 Use of Email

- a. Bargad will preferably use its own domain for email (depending on the availability of budgets). For the time being personal mailing accounts may be used for official correspondence with the permission of management.
- b. On securing a dedicated Bargad's domain, all employees will be required to use the official email addresses for official correspondence.

In case of Bargad's dedicated email accounts;

- All employees will be required to use the official email addresses for official correspondence.
- More than 25 MB of attachments will not be allowed with any outgoing message. The attachments bigger in size will be sent by IT Officer directly from server.
- Email account will be suspended in case any illegal activity or spamming
- Emails account will be configured with outlook at user systems/laptops. Therefore, all emails will be download/moved to their local system (outlook data files folder). These folders will be backed up by the IT Officer on a regular basis.
- Mail server will maintain backup for 14 days. Afterwards, the emails will be deleted from server.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, malware, ransomware, or

Trojan horse code, etc.

- Clean your “mail box”, “deleted items” and “share folders” regularly from files or emails that are not required or important.

3.6 Responsibilities of Employees

Employees and consultants are responsible for protecting BARGAD information assets and reputation. Each user is responsible and accountable for all activities associated with his/her Internet access account, and must protect his/her passwords accordingly. Users are responsible for the content of all files or information that they distribute.

The passwords should be changed by the users frequently at least once a month. The passwords should be complicated to make them more secure. All users should secure their passwords and should not share with other users. In case of any doubt, the users should be advised to change their passwords immediately or they can request a change if he / she feel necessary.

Managers are responsible for ensuring that staff and consultants adhere to this directive. Perceived productivity issues should be addressed directly to employees. Manager suspecting violation of BARGAD’s policy or a misuse / abuse of BARGAD Internet services must take appropriate action.

3.7 Maintenance of Computer Systems

- a. It is the responsibility of IT section to maintain all computer systems in BARGAD.
- b. For Hardware related maintenance BARGAD may enter into a maintenance agreement with vendors, if needed.
- c. For any hardware related problems users are instructed to inform IT Officer who will register such complaint with vendor and will arrange a backup equipment if such repair requires more than 24 hours.
- d. All software related problems shall be dealt in house by IT Officer. He/she will also maintain a maintenance record for each computer, printer and related equipment in BARGAD.
- e. He/she will do quarterly servicing of computer systems.
- f. He /She is also required to regularly download updates for licensed software’s, clean temporary and log files from user systems and defrag their systems on regular basis and help users to organize their data systematically.

3.8 Disaster Recovery Plan

(any procurements involved are dependent upon the availability of budgets)

To meet emergencies situation every office IT/Operations department will be responsible for chalking out a disaster recovery plan and its implementation. The main purpose of this plan should be to turn the disaster state into normal within shortest possible time and to protect all critical data loss.

A computer system shall be prepared as a backup server. It shall be the duty of IT Officer to keep all data updated in that backup server. The server should be in ready state with all internet, exchange server, Antivirus server and SQL server services. The attempt should be made to install a separate Hard Disk in working main server for all type of official Data. A separate back up of all critical data shall be taken on daily basis and after recording it on a DVD, it will be placed in Finances Cash Safe (which is fireproof).

Upon occurrence of any disaster that causes interruption of service or complete failure of network service, IT Officer will immediately, switch the network to back up server, and for doing this either he will install the Hard Disk containing Data in Backup Server Machine (provided hard disk is saved) otherwise restore data from DVD on local hard disk of backup server. After booting the server machine and starting all services. He/she will confirm that all systems are properly joined/logged-in with the back server, starting from Executive Director, Finance, and then other office staff members.

In case of occurrence of disaster, the recovery time should not be more than two hours in case of SQL servers and one day for other computers/server machines. As given above the backup schedule shall also help in recovery of data. All final backup data should be placed in Cash Safe, and a copy of important data written on CDs/DVDs can be given to the Director Operations to place at her home place.

Other offices should keep the all-important /critical data backup saved on a CD/DVD and give it to their respective office in-charges to place at their home.

3.9 Security of Data

The staff is expected not to share the official data/information with any other person unless it is specifically authorized to do so.

All data/files will be copied to the shared network folder marked on each user machine by the IT officer. IT officer will regularly copy and back up the data from these specific locations for later retrieval as and when required. One additional copy will be secured on external hard-drives on monthly basis.

Bargad will purchase space on the cloud where one additional copy of data will be secured. Users will be responsible for any loss of data in the event that it is copied in the specific folder.

Antivirus, anti-malware and anti-ransomware will be installed on machines for enhanced data security. IT Officer will be responsible for the regular updates of this software.

3.10 Security of Server Machines

All server machines will be secured in an isolated space where temperature and humidity levels will be maintained as required by the equipment installed. The space provided will be equipped with fire extinguishers and fire alarms. The space will be locked and entry of un-authorized personnel will be strictly prohibited. A notice will be pasted on a visible place near the entry point of the place so mentioned.

3.11 Database/Software credential and backup

Database user names and passwords are confidential. Only IT Officer and the related director (s)/manager (s) will keep such passwords. IT Officer will back up the database on a daily, weekly and monthly basis. One copy of backup should be placed on other external storage drive. One copy of backup will also be written on external disk and will be handed over to director operations for retrieval as required.

3.12 IT- Person Substitution

In absence of the IT Officer, the Director Operations or the person designated by the management will be his/her representative who will be succeeded with. In the absence of director operations, the executive director will handle the situation

3.13 Administrative Guidelines

(any procurements involved are dependent upon the availability of budgets)

- a. The IT Officer will prepare troubleshooting guidelines for employees.
- b. NEVER Install user level applications on BARGAD's Main Server and Accounts Server.
- c. Install Licensed Software on BARGAD Servers.
- d. Regularly download and install updates of Windows and Antivirus product.
- e. Document all Servers configuration / settings and keep a record of changes.
- f. Maintain regular monitoring schedule for BARGAD Network and Servers.
- g. Provide short term trainings / assistance to BARGAD Staff.
- h. Provide a copy of confidential passwords to the Executive Director. The IT department is responsible for the administration of IT Security Policies.
- i. IT Officer will ensure that all the machines are protected using proper UPS or backup power supply.

3.14 General Guidelines

The users are expected to ensure that they will follow the general guidelines as given below:

- a. NEVER use any workstation in the absence of related person without his/her permission. In exceptional cases, permission from the head of department will; be required.
- b. As per the policy we do not recommend to define their local hard drives and / or full partitions as a shared resource. This will prevent unauthorized access to applications and data.
- c. Users should not change the resource sharing policy without IT Officer's permission like sharing folders, printers or other shared devices.

- d. Any BARGAD related Data (include Backups) will not be allowed to be taken outside BARGAD premises unless it is specifically allowed by relevant Section Head or Executive Director.
- e. NEVER copy confidential files like budgets, financial statement, appraisals etc. in share folders due to confidentiality.
- f. NEVER disclose your Windows Login passwords to others. Passwords should not be recorded where they may be easily obtained.
- g. BARGAD User will not see and / or promote any porn and/or offensive materials. In such a case, the matter will be referred to the disciplinary committee for appropriate action.
- h. Users will not peep into the other's screens/monitors.
- i. No employee will misuse, disclose without proper authorization, or alter the information stored on any other's computer.
- j. Any conduct that would constitute or encourage a criminal offense, leads to civil liability, or otherwise violates any regulations, local, state, national or international.
- k. Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.
- l. Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- m. Any form of gambling is strictly prohibited.
- n. The laptop users are advised to secure their laptops under lock and key before leaving the office. Also, they should unplug the chargers when the batteries are charged or before leaving the office
- o. All users are advised to keep the food item/drinks asway from the machines