TRANSPARENCY INTERNATIONAL BANGLADESH

Social movement against corruption

INFORMATION TECHNOLOGY POLICIES & PROCEDURAL MANUAL

With Effect from 1st July 2017

www.ti-bangladesh.org

Introduction

Over the past years, Transparency International Bangladesh (TIB) has significantly grown both programmatically and institutionally. We have the distinction of being the largest chapter of TI in the world implementing multi-dimensional and robust programmes. This means that we are handling larger and newer resources, projects, staffs, partner and vendors. With this growth, the policies and procedures related to Transportation and travel have required updating and amendments to ensure the high standards of transparency and accountability that TIB is known for, and is expected to be. Our main objective is to ensure that our transportation and travel procedure and all actions, decisions and activities related to it represent highest standards of economy, efficiency and effectiveness.

What follows here is the amended, updated version and combination of TIB Information Technology Policies and Procedural Manual approved by the Board of Trustees of TIB at its 92nd meeting held on 13 June 2017. All relevant members of the staff at all levels and locations are expected to be conversant with the provisions of this manual and to fully comply with the same. The Board and management hope that the policy will be fully enforced without any exception so that the underlying responsibility and accountability framework are strictly observed.

Dr. Iftekharuzzaman
Executive Director

Table of Contents

This contents intentionally left blank

This contents intentionally left blank

This contents intentionally left blank

This contents intentionally left blank

Overview

This document serves as a rulebook to ensure the proper utilization of IT resources of Transparency International Bangladesh (referred to hereafter as "TIB"). These resources are allocated only for activities that support TIB's mission, vision, goal and official activities. Any misuse, misappropriation, negligence, deliberate or disobedience concerning this document will not be tolerated in any circumstances. The right to use TIB's IT resources may be revoked if misused or abused. Any attempt to violate the provisions of this document may result in disciplinary action.

This document comprises the following policies:

- Acceptable Usage & Access Policy
- IT Security Policy
- IT Service Operation Policy
- Data Center Policy
- Business Continuity and Disaster Recovery Policy

It is the responsibility of management of TIB to implement these policies and of each individual staff member to adhere to them.

Purpose

In order to support the official activities of TIB, the Information Technology unit will provide proper IT support to and maintain the organization's backbone network and related equipment, administrative and application servers, Email and web servers, computing facilities, and institutionally-owned desktop and laptop computer systems.

The purpose of this document is to:

- Ensure the appropriate use of IT resources provided for use.
- Protect the privacy and integrity of data stored on TIB network.
- Mitigate the risks and losses from security threats to computer and network resources and compromises of network systems.
- Reduce interruptions and ensure a high availability of an efficient network essential for sustaining the business of TIB.
- Encourage users to understand their own responsibility.
- Establish controls for protecting TIB's information and information systems against theft, abuse and other forms of harm and loss.
- Ensure that TIB is capable of continuing its services even if major security incidents occur.
- Ensure the availability and reliability of the network infrastructure and the services supplied and operated by TIB.
- Ensure flexibility and an acceptable level of security for accessing information systems from the external network of TIB.
- Coordinate and carry out the activities and processes required to deliver proper IT support & services to Users.

- Maintain a secure, safe environment and must be followed by individuals working in or visiting the Data Centers.

Ownership

Any IT materials or electronic communications address, site, number, account, or other identifier associated with TIB or any unit of TIB, or assigned by TIB to individuals, units, or functions of TIB, is the property of TIB.

Coverage

The regulations described in this document apply to:

- Users refer to as such individuals or groups nominated by TIB with extended access privileges to computers and network resources of TIB.
- IT systems and/or administered by the staffs of IT unit of TIB.
- Entire IT system of TIB including server, desktop, laptop, multimedia projector, ups, modems, computer hardware & network accessories and software in TIB head office and field offices.

Adherence to the Policy

Use of IT resources at TIB is considered an agreement to abide by this policy. Violations of this policy may result in the immediate suspension of computer account and network access pending investigation of circumstances. Serious violations of the policy will be referred directly to the Executive Director; unauthorized use of TIB computers can be a criminal offense. Infractions may result in disciplinary action, up to and including termination of employment and/or criminal prosecution.

Policy Amendment

The EMT is authorized to interpret and clarify any provisions of this policy and develop/design/amend process, procedures, forms and formats required for smooth implementation of policy. Any gross amendment of this document shall be made by the Board. If any change is needed in these areas, DFA will propose to modify existing policies through EMT and upon approval of the Board of Trustees, they will be amended. DFA will communicate the changes to the employees as and when they occur.

Section 1: Acceptable Usage & Access

1. Guiding Principles: Protection and Limitations of Electronically Held Information

Data and information stored, processed and/or communicated within the IT environment of TIB belongs to TIB and is, therefore, subject to management scrutiny, which may include methods such as interception, monitoring, logging, and inspection. Audits will be conducted in order to protect the interest of TIB as well as the User. Under normal circumstances, the IT Unit will not examine personal information transmitted over the network or stored on TIB-owned computers. However, the IT Unit reserves the right to monitor system resources, including activity and accounts when:

- Necessary to protect the integrity, security, or functionality of TIB IT resources
- An account or system is engaged in unusual or excessive activity
- It has good cause to believe that the Community Principles and Practices, rules outlined in this document, or the laws of the land are being violated.

Additionally, the normal operation and maintenance of TIB IT resources requires the backup of data, the logging of activity, the monitoring of general usage patterns and other such activities as may be necessary in order to provide desired services.

Users should at all times apply the relevant security mechanisms applicable to systems under their custody.

Confidentiality should be observed when an alleged violation occurs, e.g. apparent visit to a pornographic website. Sometimes this can be accidental, or material can enter someone's computer as unsolicited Email. Proper care should be taken to protect innocent colleagues. Training, education and awareness-building should receive top priority.

1.1 IT Service Delivery

For the purpose of IT service delivery efficiency, remote access and remote desktop software may be utilized by the IT Unit to access, manage and support Users' computers remotely with the consent of the owner of computing device.

2. Compliance

Information technology resources should not be used for illegal or harmful purposes, including:

- The electronic resources should be used for the purpose for which they are intended.
- TIB network and computing resources are not allowed for personal purposes until/unless management approval.
- All computers residing on the internal TIB network, whether owned by the employee or TIB, shall be continually executing approved virus-scanning software with a current, up-to-date virus database.
- All passwords used to access TIB's IT systems must be kept secure and protected from unauthorized use.

- No user account can be shared between individuals. Authorized users are responsible for the security of their own passwords and accounts.
- Intentional destruction or damage to IT equipment, software or data.
- Intentional disruption or unauthorized monitoring of electronic communications.
- Software used in IT resources of TIB should only be installed by the IT Unit. It is the IT Unit's role to load software on computers. Use TIB installed software and hardware only.
- To ensure that major software TIB uses is properly licensed, and in order to protect users from software that may compromise TIB security (for instance, virus infections) or which may cause computer failures due to non-compatibility with our existing technology; no software should be downloaded or installed without prior consultation and approval by the IT Unit.
- The downloading and installation of screensaver software is generally prohibited because they contain a high risk of virus infection and may lead to general computer problems. Software that can be used to download illegal software is prohibited.
- Users should at all times apply the relevant security mechanisms applicable to systems guided by IT policy under their custody.
- Users must verify technical specification of IT resources from IT Unit prior purchasing any IT resources by TIB Standard specification provided by the IT Unit should be followed by Users.

2.1 Protection of IT Facilities

- User must submit signed filled-up laptop agreement form to IT unit in applicable areas.
- User must submit approved requisition form to IT unit in order to receive IT equipment from IT Pool or receive IT facilities for program venue.
- Users should not interfere with, interrupt or obstruct the ability of others to use the network or other IT resources.
- Users should not provide, assist in or gain unauthorized access to TIB computing or network resources
- Users should not attempt to circumvent or defeat computer or network security measures. Users should not bypass or attempt to bypass any information security systems like routers/firewalls of TIB. Exercise of "Onion Routing" is prohibited. Users should not use a modem or wireless access device to bypass the TIB network to connect to the Internet or external networks other than TIB while simultaneously connected to the TIB network. It leads to significant security risk to the IT assets of TIB and is, therefore, strictly prohibited.
- Users should seek permission from the IT Unit to connect personally owned computers to the TIB network.
- Users should not change any configuration of IT resources by him/her as it may impact IT systems and the network. It is the IT Unit's role to configure IT resources.
- Administrative privilege of IT resources should only be with the IT Unit, which ensures disabling the ability of Users to change the configuration.
- Users should at all times take proper care of equipment entrusted to them, which includes protection against theft, damage as a result of manhandling or poor transportation, improper

storage at inappropriate temperature and exposure to magnetic fields or adverse weather conditions.

- Nobody is authenticated to open the parts of computer and take away any hardware outside the office/workstation without the permission of IT unit.
- Staff should properly shutdown their CPU, Monitor and UPS while departing from office or not be available in sit for twenty minutes.
- Keep away tea, coffee, water or any other liquid apart from computer.
- Check pen-drive, CD or floppy disk by anti-virus software before using them.
- Game/Movie playing in computer is strictly prohibited.

2.2 Account Usage

Users of TIB are provided with a user account to access IT resources, facilitated by the IT Unit. Following is the user account usage policy:

- Account holders should use only their own user accounts. Account holders should not allow others to use their personal accounts. The person holding an account is responsible for its use, and all activity originating from that account, at all times.
- Account holders should protect their passwords and keep them confidential. Passwords should be changed frequently. Any problem resulting from irresponsible use of a password (e.g., a password that can be easily guessed or oral or written dissemination of a password) may be treated as grounds for action against the account holder. Any attempt to determine the passwords of other Users is strictly prohibited. Account holders are also responsible for ensuring that passwords meet the following minimum requirements:
- Contain characters from three of the following four categories:
    - English uppercase characters (A through Z),
    - English lowercase characters (A through Z),
    - Base 10 digits (0 through 9),
    - Non-alphanumeric characters (e.g., !, $, #, %) and
    - Be at least eight characters in length;
    - Be changed at least every 90 days.
- To further improve security, passwords should not:
    - Contain all or part of the User's account name;
    - Use a password that is personal, such as names, places colors or birth dates.
- Users should logout when they leave their workstation for twenty minutes. Alternatively Windows workstations may be locked.
- Account holders should not abuse any communications system, either local or remote, by sending rude, obscene or harassing messages or by using these systems for nonessential purposes during the times when the computers are in heavy demand. Users should not participate in the creation and sending of chain Emails. Account holders should identify themselves clearly and accurately in all electronic communications, and there should not be anonymous postings by Users. Unofficial mass Emailing (i.e., spam) are prohibited. Users should

not subscribe this Email to posts that have no official relevance. Users should avoid sending messages with bulky attachments to large audiences via distribution list.

- Account holders should use only their own files, those that have been designated as public or those that have been made available to them with the knowledge and consent of the owner.
- Respective user should use their own network folder for important official data storage purpose.
- For placing any type of image or video or clipart files in any folder of the Server then contact IT as deem appropriate.
- Staff should user their own "user ID" and "Password" to login in respective user's account.

3. Use of Email and Internet

3.1 General Use of Email

Users should take as much (if not more) care in the preparation of Emails as Users do when writing letters or faxes. Improper statements sent in Emails may give rise to personal or TIB liability, even if only sent internally. Always work on the assumption that Email messages may be read by people other than the intended recipient, and that Email they can be considered to be part of the permanent record.

Users should not send trivial or inappropriate Emails (such as chain letters) and only copy messages to people who need to read them. Otherwise, Users will compromise the purpose of having the system, namely the fast and efficient transfer of information. Users should zip any attachments they send outside TIB. Users are allowed to send attachment of 15 MB with email.

Users must immediately report to the IT Unit any actual, suspected or threatened occasions they encounter regarding Emails being intercepted or tampered with, or being sent or received contrary to the policies contained herein.

3.2 Prohibited Use

User must not send Emails that are abusive, sexist, racist, discriminatory, defamatory, obscene or otherwise likely to cause offence.

- Abusive Emails are likely to amount to harassment, as are repeated and unwanted Emails requesting a date, containing sexual innuendo or remarks or simply pestering the recipient on non-work-related matters. It is the effect on the recipient that is important, not whether the User intends to cause offence.
- The same considerations apply to issues concerning racial harassment.
- Users should avoid sending messages with image attachment to large audiences via distribution lists during festival time.
- Defamatory statements sent by Email, either externally or internally, could cause legal liability to both User and TIB, and a claimant may be able to bring legal action in any country where the message is read.
- The creation, dissemination, storage and display of obscene or pornographic materials.

- The creation, dissemination, storage and display of drama/movie/music/videos those are not relevant to TIB activities.
- The creation, dissemination, storage and display of defamatory materials or materials likely to cause offence to others.
- Voice chatting by Skype or other software is not allowed without management approval.
- Playing game, browsing website of job portals/stock exchange/social networking including facebook, twitter, youtube, etc. are not allowed in official computers without management approval.
- Do not browse websites that are not related to TIB purpose.
- Using any type of Chatting software (like Yahoo Messenger, MSN Messenger, etc.) is prohibited.
- Browsing adult sites, gaming sites are totally banned and considering being violation of TIB Code of Ethics.

TIB acknowledges that it may not be possible to control receipt by Users of offensive material from external sources; Users are, however, accountable for passing to others any material they receive. Please refer to the Account Usage Policy and Guiding Principles section for further details.

3.3 Personal Use

Users are permitted to attend to personal matters by Email during working hours, but this personal use should not be excessive and should not interfere with User's job performance, nor should it interfere with the performance of TIB's systems.

Access to personal use of Email may be limited due to IT constraints. Users should not use the system for inappropriate purposes, for example to send chain letters, or for any of the "prohibited uses" outlined above.

3.4 Employee's Responsibility to Protect TIB's System from Viruses

Computer viruses pose a significant threat to the stability of IT systems of TIB, and it is the responsibility of every User to minimize the risk of their introduction.

Any Email received with a non-text file attachment (which may be contained within a zipped file attachment) must be deleted unless it is clearly identified as being work related. If Users have any suspicions about a file attachment, in particular a non-text attachment, they should refer it to the IT Unit before opening it.

Any Email that Users receive warning of potential viruses should be forwarded to the IT Unit, not circulated to "everyone".

3.5 Legal Liability

User should always remember that, when s/he creates an Email, s/he is creating a document; it may be required to be disclosed in any court proceedings, or as a result of investigations carried out by authorities. Email messages are not automatically destroyed, even after they have been "deleted", and it can be illegal to attempt to do so.

Users must take care to avoid entering into legal relations or contractual commitments with third parties by Email. It is important that you do not make statements by Email in pre-contract negotiations that are incorrect and could give rise to claims for misrepresentation, and that Users do not attempt to conclude contracts by Email.

User should not alter someone else's Email and forward it without highlighting his/her alterations, as this could amount to misrepresentation.

3.6 Guidance on Use of the Internet

Employees have been given access to the Internet as a tool to support their work. At no time may users use TIB equipment to access illegal, immoral or otherwise inappropriate sites, in particular sites with pornographic or on-line betting/gambling content. If Users enter any of these sites by accident, they should leave the site immediately.

4. Disciplinary Warning

TIB will carry out an investigation if there is a complaint of misuse of IT systems (including misuse of Email and/or the Internet), or if TIB suspects an employee has been misusing the system.
TIB expressly reserves the right to access the employee's device supplied by TIB (computer, laptop, netbook, etc.) to investigate such a complaint or to make available the employee's device supplied by TIB to an external IT adviser to carry out the necessary investigations. TIB reserves the right to suspend employee from employment to allow the necessary investigations to be carried out. Any misuse of the system will result in disciplinary action (up to and including summary dismissal) being taken against employee, in accordance with TIB's disciplinary procedure.

Section 2: IT Security

This page intentionally left blank

This page intentionally left blank

This page intentionally left blank

This page intentionally left blank

This page intentionally left blank

This page intentionally left blank

This page intentionally left blank

This page intentionally left blank

This page intentionally left blank

Section 3: IT Service Operations

1. IT Helpdesk

The IT Helpdesk is the primary point of contact for Users when there is a service disruption, for service requests or even for some categories of Request for Change. The IT Helpdesk provides a point of communication to the Users and a point of coordination for several groups and processes.

The IT Helpdesk is a vitally important part of the IT Unit and should be the single point of contact for IT Users on a day-by-day basis – and will handle all incidents and service requests.

1.1 IT Helpdesk Scope

The primary aim of the IT Helpdesk is to restore the "normal service" to the Users as quickly as possible. In this context, "restoration of service" is meant in the widest possible sense. While this involves fixing a technical fault, it equally involves fulfilling a service request or answering a query – anything that is needed to allow the Users to return to working satisfactorily. Specific responsibilities will include:

- Logging all relevant incident/service request details, allocating categorization and prioritization codes
- Providing first-line investigation and diagnosis
- Resolving those incidents/service requests as they are able
- Escalating incidents/service requests that they cannot resolve within agreed timescales
- Keeping Users informed of progress
- Closing all resolved incidents, requests and other calls
- Conducting customer/User satisfaction callbacks/surveys as agreed
- Communication with Users – keeping them informed of incident progress, notifying them of impending changes or agreed outages, etc.

Usually, the IT Helpdesk of TIB works within office hours.

2. Event Management

Event Management monitors all events that occur throughout the IT infrastructure, to monitor normal operation and to detect and escalate exception conditions. The IT Unit is responsible for event management for IT resources.

2.1 Scope

Event Management may be applied to any aspect of Service Management that needs to be controlled and which may be automated. These include:

- Some configuration Items will be included because they need to stay in a constant state (e.g. a switch on a network needs to stay on and Event Management tools confirm this by monitoring responses to "pings").

- Some configuration Items will be included because their status needs to change frequently and Event Management may be used to automate this and update the Configuration Management System (e.g. the updating of a file server).
- Environmental conditions (e.g. fire and smoke detection)
- Software license monitoring for usage to ensure optimum/legal license utilization and allocation
- Security (e.g. intrusion detection)
- Normal activity (e.g. Tracking the use of an application or the performance of a server).

2.2 Process Activities, Methods and Techniques

IT Unit should follow the process of activities regarding event management. Each activity in this process is described below:

2.2.1 Event Occurs

There are many different types of events, those are detected or registered by the IT Unit.
Events not limited to the following are detected or registered:

- Events that signify regular operation:
- Notification that a scheduled workload has been completed.
- A User has logged in to use an application.
- An Email has reached its intended recipient.
- Events that signify an exception:
- A User attempts to log on to an application with the incorrect password.
- An unusual situation has occurred in a business process that may indicate an exception requiring further business investigation.
- A device's CPU is above the acceptable utilization rate.
- Events that signify unusual, but not exceptional, operation. These are an indication that the situation may require closer monitoring. In some cases, the condition will resolve itself, for example in the case of an unusual combination of workloads – as they are completed, normal operation is restored. In other cases, operator intervention may be required if the situation is repeated or if it continues for too long. These rules or policies are defined in the Monitoring and Control Objectives for that device or service.

Examples of this type of event are:

- A server's memory utilization reaches within 5% of its highest acceptable performance level.
- The completion time of a transaction is 10% longer than normal.

2.2.2 Event notification

Event notifications may be proprietary, in which case only the manufacturer's management tools may be used to detect events. Configuration Items may generate event notifications using an open standard such as SNMP (Simple Network Management Protocol).

2.2.3 Event detection

Once an event notification has been generated, it is detected by an agent running on the same system, or transmitted directly to a management tool specifically designed to read and interpret the meaning of the event.

2.2.4 Event Filtering

The purpose of filtering is to decide whether to communicate the event to a management tool or to ignore it. If ignored, the event will be recorded in a log file on the device, but no further action will be taken. During the filtering step, the first level of correlation is performed, i.e. the determination of whether the event is informational, a warning or an exception (see next step).

2.2.5 Significance of Events

Categorization of the significance of an event is as follows:

- **Informational:** This refers to an event that does not require any action and does not represent an exception. They are typically stored in the system or service log files and kept for a predetermined period. Informational events are typically used to check on the status of a device or service, or to confirm the successful completion of an activity. Informational events can also be used to generate statistics (such as the number of Users logged on to an application during a certain period) and as input into investigations (such as which jobs completed successfully before the transaction processing queue hung).
- **Warning:** A warning is an event that is generated when a service or device is approaching a threshold (e.g. memory utilization on a server, collision rate on a network). Warnings are intended to notify the appropriate person, process or tool so that the situation can be checked and the appropriate action taken to prevent an exception. Warnings are not typically raised for a device failure.
- **Exception:** An exception means that a service or device is currently operating abnormally.

2.2.6 Event Correlation

If an event is significant, a decision is made to determine the level and type of business impact, what the significance is and what actions need to be taken to deal with it.

2.2.7 Trigger

If the correlation activity recognizes an event, a response is required. Trigger is the mechanism used to initiate that response.

2.2.8 Response Selection

Response options are as follows and may be chosen in any combination:

- **Event logged:** The event is logged as an Event Record in the Event Management tool or it may be as an entry in the system log of the device or application that generated the event. IT Operations staff checks the logs on a regular basis.

- **Auto response:** Some well-understood events results in Problem Management are automated. The trigger will initiate the action and then evaluate whether it was completed successfully.
- If not, an Incident or Problem Record will be created.
- **Alert and human intervention:** When an event requires human intervention, it will be escalated. The purpose of the alert is to ensure that the person with the skills appropriate to deal with the event is notified. The alert will contain all the information necessary for that person to determine the appropriate action.
- **Incident, problem or change:** In a certain situation, appropriate event response will be needed to be handled through the Incident, Problem or Change Management process. These are described in the incident and problem management process in this policy.

2.2.9 Review actions

In the cases where events have initiated an incident, problem and/or change, the Review will ensure that incidents, problems or changes originating within Operations Management do not get lost between the teams or departments. The Review will also be used as input into continual improvement and the evaluation of the Event Management process.

2.2.10 Close Event

In the case of events that generate an incident, problem or change, these should be formally closed with a link to the appropriate record.

3. Incident Management

3.1 Purpose

The primary goal of the Incident Management process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

3.2 Scope

Incident Management includes any event which disrupts a service. Incident Management is the process for dealing with all incidents; this can include failures, questions or queries reported by the Users (usually via a telephone call to the IT Helpdesk), by technical staff, or automatically detected and reported by event monitoring tools.

3.3 Process Activities, Methods and Techniques

IT Unit should follow the process of activities regarding incident management. Each activity in this process is described below:

3.3.1 Incident Identification

When an incident has occurred, a User is affected and contacts the IT Helpdesk. As far as possible, all key components should be monitored so that failures or potential failures are detected early so that the

incident management process can be started quickly. Ideally, incidents should be resolved before they have an impact on Users.

3.3.2 Incident Logging

All incidents should be fully logged and date/time stamped, regardless of whether they are raised through the IT Helpdesk telephone call or whether automatically detected via an event alert. If the IT Helpdesk and/or support staff visits the User to deal with one incident, they may be asked to deal with further incidents while they are there. It is important that, if this is done, a separate Incident Record is logged for each additional incident handled – to ensure that a historical record is kept and credit is given for the work undertaken. All relevant information relating to the nature of the incident should be logged so that a full historical record is maintained – and so that, if the incident has to be referred to the IT Unit, they will have all relevant information to assist them. The information in each incident may include:

- Unique reference number
- User details
- Equipment details
- Date/time initially logged
- Priority and categorization details
- Incident description
- Details of all diagnostic or attempted recovery actions taken
- Activities undertaken to resolve the incident
- Resolution date and time

3.3.3 Incident Categorization

During incident logging, incident categorization should be done so that the exact type of the call is recorded. The categorization of the incident should be checked, and updated if necessary, at call closure time.

3.3.4 Incident Prioritization

During logging, every incident should be prioritized – as this will determine how the incident is handled both by support tools and support staff. Prioritization is determined by taking into account both the urgency of the incident (how quickly the business needs a resolution) and the level of impact it is causing. An indication of impact is often (but not always) the number of Users being affected. The loss of service to a single User can have a major business impact – it all depends upon who is trying to do what – so numbers alone is not enough to evaluate overall priority. Other factors that may also contribute to impact levels are:

- The number of services affected – may be multiple services
- The level of financial losses
- Regulatory or legislative breaches

3.3.5 Initial Diagnosis

When incident is routed via the IT Helpdesk, the IT Helpdesk person should carry out initial diagnosis, typically while the User is still on the telephone, try to discover the full symptoms of the incident and determine exactly what has gone wrong and how to correct it. If possible, the IT Helpdesk person will resolve the incident while the User is still on the telephone and close the incident if the resolution is successful. If the IT Helpdesk person cannot resolve the incident while the User is still on the telephone, but there is a prospect that the IT Helpdesk may be able to do so within the agreed time limit without assistance from other IT support groups, the person should inform the User of this intention, give the User the incident reference number and attempt to find a resolution.

3.3.6 Incident Escalation

- **Functional Escalation:**

  As soon as it becomes clear that the IT Helpdesk is unable to resolve the incident itself or when target times for first-point resolution is exceeded, the incident must be immediately escalated for further support. The IT Unit has a second-level support group (Application/ERP Development Team, System and Infrastructure Team), and the IT Helpdesk should refer the incident to them, as the incident will need deeper technical knowledge. When the second-level group has not been able to resolve the incident within agreed target times, the incident must be immediately escalated to the appropriate third-level support group. Third-level support groups may also be third parties, such as software suppliers or hardware manufacturers or maintainers. Incident Ownership remains with the IT Helpdesk at all times. The IT Helpdesk remains responsible for tracking progress, keeping Users informed and ultimately for Incident Closure.

- **Hierarchic Escalation:**

  If incidents are of a serious nature, the SM of IT Unit must be notified, for informational purposes at least. Hierarchic escalation is also used if the Investigation and Diagnosis and Resolution and Recovery steps are taking too long or proving too difficult. Hierarchic escalation should continue up the management chain so that senior managers are aware and can be prepared and take any necessary action, such as allocating additional resources or involving suppliers/maintainers. The IT Helpdesk should ensure the Incident Record is updated accordingly to keep a full history of actions.

3.3.7 Investigation and Diagnosis

In the case of incidents where the User is just seeking information, the IT Helpdesk resolves the service request, but if a fault is being reported, some degree of investigation and diagnosis is required. Each of the support groups involved with the incident handling will investigate and diagnose what has gone wrong and all such activities (including details of any actions taken to try to resolve or re-create the incident) should be fully documented in the incident record so that a complete historical record of all activities is maintained at all times.

3.3.8 Resolution and Recovery

When a resolution of an incident is found, sufficient testing should be performed to ensure that recovery action is complete and that the service has been fully restored to the User(s).The recovery actions depending upon the nature of the fault may involve:

- Asking the User to undertake directed activities on his/her own computer or remote equipment
- The IT Helpdesk implementing the resolution either centrally (say, rebooting a server) or remotely using software to take control of the User's desktop to diagnose and implement a resolution
- Specialist support groups being asked to implement specific recovery actions
- A third-party supplier or maintainer being asked to resolve the fault
- In some cases, two or more groups may take separate, though perhaps coordinated, recovery actions for an overall resolution to be implemented. In such cases, Incident Management must coordinate the activities and liaise with all parties involved. Regardless of the actions taken, or who does them, the Incident Record should be updated accordingly with all relevant information and details so that a full history is maintained. The resolving group should pass the incident back to the IT Helpdesk for closure action.

3.3.9 Incident Closure

The IT Helpdesk should check that the incident is fully resolved and that the Users are satisfied and willing to agree that the incident can be closed.

The IT Helpdesk should also check the following:

- **Incident documentation:**
  Chase any outstanding details and ensure that the Incident Record is fully documented so that a full historic record at a sufficient level of detail is complete.
- **Ongoing or recurring problem:**
  Determine (in conjunction with resolver groups) whether it is likely that the incident could recur and decide whether any preventive action is necessary to avoid this.
- **Formal closure:**
  Formally close the Incident Record.

4. Request Fulfillment

Request Fulfillment is the process for dealing with Service Requests – changes – initially via the IT Helpdesk, but using a separate process similar to that of Incident Management but with separate Request Fulfillment records with approval. Necessary linked to the Incident or Problem Record(s) should be present if that initiates the need for the request.

Section 4: Data Center

This page intentionally left blank

This page intentionally left blank

This page intentionally left blank

Section 5: Business Continuity/Disaster Recovery

This page intentionally left blank

This page intentionally left blank

This page intentionally left blank

This page intentionally left blank

This page intentionally left blank

This page intentionally left blank

This page intentionally left blank

This page intentionally left blank

This page intentionally left blank

This page intentionally left blank

Section 6: Procedure and Others

1. Emergency Operating Procedure

In the event of an emergency, normal operating procedures should be restored as quickly as possible. Due to the small size of our department, it is beneficial that all employees learn laterally to allow for greater ability to maintain operations should any individual employee be unavailable. The steps below will indicate how operations should continue in the event of an emergency directly affecting the TIB's IT unit.

1. Assess situation and determine the impact to the IT system and report to Director, F&A, with no delay.
2. Determine if any equipment loss has occurred. If so, proceed to step 3. If not, proceed to step 5.
3. Determine what resources are affected and bring them back up as soon as possible:
    - Network and connectivity equipment
    - Mission critical services.
    - Non-mission critical services.
4. Once all connectivity and resource shave been restored, normal operations can now resume.
5. Complete documentation of handled situation.

2. IT Requisition Procedure

This document is to serve as a set of guidelines for all TIB staffs who choose to request IT requisition for event support/field visit:

- Staffs are expected to use "TIB's Venue and IT Equipment Requisition Form" for IT requisition.
- Requisition form need to filled-up properly with appropriate information.
- IT unit shall provide equipment based on availability and first-come-first-serve basis.
- Staffs are expected to collect voice/camera picture/ laptop data from respective device immediately after end of the event/field visit by own responsibility.

3. IT Equipment Purchase Procedure

This document is to serve as a set of guidelines for all TIB staffs who want to purchase IT equipment:

- End user should submit their request to IT unit for purchase.
- IT unit collect necessary information regarding price, brand, model, etc. from potential vendors through procurement unit.
- IT unit then submit "Purchase Request" to procurement unit for next step of processing. Procurement unit must follow the procurement process according to TIB's procurement manual.
- IT unit must use TIB's official "PR" form and include "Note for record" in appropriate areas.
- After receiving products, IT unit shall provide IT equipment to end user with appropriate configuration done.

Section 7: Forms

7.1 TIB's Venue and IT Equipment Requisition Form

Transparency International Bangladesh (TIB)
TIB's Venue and IT Equipment Requisition Form

Date:
Purpose:

Required venue (Please mark):

Meghomala ☐	**Udoypadma** ☐	**Meeting Room** ☐ (5th floor)	**Meeting Room** ☐ (4th floor)
Others (Please specify):			

Date of programme: **Time of Programme:**
Duration (Please specify):

Short period			Half day		Full day
From: am/pm		To: am/pm	1st half ☐	2nd half ☐	☐

Appox. no. of participants:
Logistical support (if any):
Required IT Materials(Please mark):

					For use in venue	Others
Multimedia Projector	☐	**Laptop**	☐	**Projection Screen**	☐	
Speaker	☐	**Voice Recorder**	☐	**Printer**	☐	
Still Camera	☐	**Video Camera**	☐	**Modem**	☐	
Others (specify if needed):						

Requested by:

Signature:
Name:
Designation:
Division/Unit:

Approved by SPM/Divisional Director:

Signature:
Name:
Designation:
Division/Unit:

User's will submit approved request- original to Admin and copy to IT

For the use of Administration	**For the use of IT Unit**
Venue Allocated by:	**Checked by Requisition Sl. No.** **Signature:** **Name:**
Name of staff assigned for the programme:	**Designation:**
Signature of Admin Manager: **Remarks (if any)**	**Remarks (if any)**

7.2 Laptop Agreement Form

FULL TIME LAPTOP AGREEMENT FORM

This agreement is made and signed on ……..…. Day of …….at containing additional terms agreed by

BETWEEN

Transparency International Bangladesh (TIB)

AND

Mr/Ms/Mrs……Designation……..EIN……
Present Address……..…….
Permanent address……...is treated as an individual.

Whereas Transparency International Bangladesh. Term used as “TIB” as "Provider" is providing a laptop to an individual as "Recipient" for official purpose.

Now, in consideration of the use of the assets, the employee covenants as here under;

I undertake:

- To take proper and reasonable care of the asset at all the times, will not misuse the same and take all necessary and adequate safeguard to protect the asset of TIB and shall not use it for any unlawful or unethical purpose. At the same time, I shall not install / use any unlawful data / software in the course of use of the asset.
- I agree not to mortgage / lien / rented or otherwise create any charges / encumbrances on the said asset of TIB, whether present or future, and will not, under any circumstances, as off the asset as my own. I further agree to return the asset on termination of my services or on leaving the services of TIB, for any reason whatsoever.
- I agree that in the event of any loss / damage to the asset, I will immediately lodge an FIR and submit the original copy to the HR and a copy at IT Unit for record. In case of the loss of laptop be it on, or off Organization premises, due to negligence of the user staff members, the Organization will recover the cost of the laptop from the user staff members. It is the Organization’s discretion to impose further penalties on account of loss of sensitive Organization information.
- I agree to submit myself to random audit by TIB IT Unit, in order to check the physical presence as well as the functional usability of the asset. I shall also abide by any recommendation of IT Unit to optimize the performance of the Laptop computers.
- To take the Laptop computer to IT Unit for checking in each after three months.
- To maintain the secrecy and the confidentiality, at all times, with respect to all the data and information relating to TIB and or used in relation to my employment with TIB, contained in the asset, whether past, present or future, in whatever form.
- The term of this agreement will be enforcing till the last day of working in the organization or till the return of the Laptop.
- In case of any difference/ dispute arising out of or in connection with the use of the asset or the terms and conditions of this agreement, the same will be referred to the Executive Director for decision on the matter.
- In case of my leaving the employment or being terminated for any reason, I will hand over the asset to TIB in good condition failing which TIB is authorized to penalty against me and which should be adjust with my final payment. In case of shortage of amount, I should deposit the rest of amount otherwise TIB can go for legal initiative against me.
- The equipment will always remain TIB’s property. I shall return the asset to TIB following the instruction of the authority at anytime if so asked.
- I acknowledge that I have read and understood the terms and conditions of this agreement and further agree to abide by all the terms and conditions set forth herein. At the same time any action can be taken by Management according the Laptop Usages Policy for any loss / damage.

Agreement accepted by (Recipient)

(Signature)

Senior Manager IT / Director F&A (Provider)

(Signature)

List of Do's and Don'ts:

All of the eligible staff member/s of Laptop and the other of TIB's Laptop user/s must be followed the following List of Do's and Don'ts:

1) Organization provided Laptop Computers are intended to be used following the Laptop Computer Usages Policy, Agreement and the organizational Information Technology guideline.

2) Do not expose Laptop Computer to any Magnetic fields (like: Mobile/Cell Phone, Magnet, near to electrical transformer, Stabilizer, UPS, high end speaker, Sound woofer etc.) that could damage the contents of the Hard disk as Laptop Computer contains a Magnetic Hard disk. Any Magnetic field will be harmful for Laptop's LCD, Hard Disk, Network card, Keyboard and all of the integrated devices.

3) Do not store batteries for long periods plugged into or attached to any power source. This includes AC adapters and laptop security carts plugged into an outlet.

4) Laptop (Lithium-ion) batteries, including those stored in laptop systems, should maintain an Operational Storage Temperature of 0° to 35°C (32° to 95°F).

5) NEVER EVER discharge the battery to below 20% capacity. So set your computer to give you a battery warning at 20%, and switch the laptop off! Laptop batteries should not be frequently fully discharged and recharged ("deep-cycled"), but this may be necessary after about every 30th recharge to recalibrate any electronic charge monitor (e.g. a battery meter). This allows the monitoring electronics to more accurately estimate battery charge. This has nothing to do with the memory effect.

6) It is highly recommend that, when the run time of laptop battery does not meet your needs, please contact with IT Unit immediately.

7) Please don't touch the screen with your hand or any other sharp object (If the screen needs to be cleaned please use soft cloth to clean it) and please don't use the laptop near liquids and do not eat or drink while using the laptop.

8) Turn Laptop Computer off and place it in its folded position any time when it is to be moved.

9) The Laptop Computer should not be taken to any third body (i.e. Laptop user's Relatives, Outside IT Personnel/experts, Computer Troubleshoot Company or any one) except Transparency International Bangladesh (TIB's) IT Unit for any types of problem (Hardware, Software or Physical) faced by the eligible user of Laptop.

10) The user should keep the Laptop in safe place and out of reach of the children or minors for safety purposes.

To be filled in by IT Unit

Date:

Asset Number: _____

Brand & Model name: _____ Value: _____

Distributed by (IT Staff): ……..

Approved by SM -IT: ……..