IT Services Policies

Version: 1.0

May 5, 2020

1. Table of Contents

2. Document Information

2.1. Approval Document

Document Name	IT Services Policies
Document Code	ITS-POL-002
Classification	Policy
Author	Owais Ahmed
Reviewer	Muhammad Saad Ullah Khan
Approver	Muhammad Shamoon Haider
Current Version	1.0
Release Date	May 5, 2020

2.2. Document History

Version Changed	Change Description	Change Approver	Approval Date & Method

3. Purpose

This document is aim to comply the ITSMS at Sybrid ITS Tech Division, and to ensure that information lies within the organization are managed, controlled, safeguarded and used in an efficient and effective manner related to different processes and practices like incident management, problem management, change management, release management, supplier management, budgeting and accounting, availability management, capacity management and others ITSM policies for services delivery and support for clients by Sybrid ITS Tech Division.

4. Scope

These policies apply to Sybrid ITS Tech Division and the clients for proper service delivery and availing the services support.

5. Policy Enforcement / Compliance

Compliance with these policies are mandatory and ITSM Steering team shall ensure continuous compliance monitoring within the Sybrid ITS Tech Division. Compliance with the statements of these policies is a matter of periodic review by ITSM Steering team. Any violation will result in disciplinary action as per the Sybrid ITS Tech Division related policy.

Disciplinary action will be depending on the severity of the violation, which will be determined by the investigations. Actions such as termination or others as deemed appropriate by the Sybrid ITS Tech Division Top Management and Human Resources Department shall be taken.

6. Policy Management and Review

Technological advances and changes in the business requirements will necessitate periodic revisions to policies. Therefore, this policy may be updated to reflect changes or define new or improved requirements.

Deficiencies within this policy shall be immediately communicated to the ITSM Steering team. This policy will be reviewed at annual basis or in case of any special event as by ITSM Steering team head discretion. Policy changes will require the approval of the ITSM Steering head.

Change log shall be kept current and will be updated as soon as any change has been made.

7. Clause Reference

- 5.1 General
- 6.4 Budgeting and accounting for service
- 6.6.2 Information security controls
- 7.2. Supplier Management Policy
- 9.2 Change Management
- 9.3 Release and deployment management

8. Abbreviations used in this document

ITS	Information Technology Services
ITSM	Information Technology Service Management
ITSMS	Information Technology Service Management System
CI	Configuration Item
CAB	Change Authorization Board

9. Incident Management Policy

To restore normal service operation as quickly as possible and minimize the adverse impact on business operations.

- Incidents shall be recorded and categorized
- Incidents shall be prioritized and analyzed

10.Problem Management Policy

To minimize the adverse impact of incidents and problems on the business that are caused by underlying errors within the infrastructure, and to prevent recurrence of incidents related to these errors. Determine the root cause of incidents and initiate actions to improve.

- Problems shall be identified, recorded and classified
- Problems shall be prioritized and analyzed
- Problems shall be resolved and closed
- Problems not progressed according to defined service levels shall be escalated

11.Change Management Policy

CAB of Sybrid ensures the following making any changes in the system;

- Changes are planned and tested before they are accepted for deployment
- Changes are checked and verified after deployment to identify and rectify any unexpected or unwanted results
- Emergency Changes are verified after deployment and measures are taken to strengthen them

12.Configuration Management Policy

The policy described how the service components (Configuration Items) have been configured and the relationships between assets management.

- All configuration items (CIs) within Service Management systems and infrastructure shall be accurately identified and relationships recorded

- The status of the CIs and modifications shall be effectively recorded, tracked, and reported
- Changes to CIs shall be controlled
- Any exceptions between configuration records and the corresponding CIs shall be identified and corrected
- The integrity of released systems, services and service components shall be assured

13.Capacity Management Policy

To ensure that capacity of IT services and the IT infrastructure meets the agreed capacity and performance related requirement in a cost effective and timely manner. Meet both the current and future capacity and performance needs of business.

- Current and future capacity and performance requirements shall be identified and agreed
- A Capacity Plan shall be developed based on capacity and performance requirements
- Capacity shall be provided to meet current capacity and performance requirements
- Capacity usage shall be monitored, analyzed and performance is tuned
- Capacity shall be prepared to meet future capacity and performance needs
- Changes to capacity and performance shall be reflected in the Capacity Plan

14.Release Management Policy

To plan, schedule and control the build, test and deployment of releases, and to deliver new functionality required by the business while protecting the integrity of existing services.

- Requirements for releases shall be established and agreed upon with affected parties
- Releases of new or changed services and service components shall be planned
- Releases shall be designed
- Releases shall be tested prior to deployment
- Approved releases shall be deployed
- Integrity of hardware, software and other service components shall be assured during deployment of the release
- Unsuccessful deployed releases shall be reversed

- Release information shall be communicated to affected parties

15.Availability Management Policy

Ensure that the level of availability delivered in all IT services meets the agreed availability needs and/or service level targets in a cost effective and timely manner. Meet both the current and future availability needs of business.

- Service availability requirements shall be identified
- A service availability plan shall be developed using service availability requirements
- Service availability shall be tested against the service availability requirements to validate the plan
- Service availability shall be monitored
- Underlying causes of unanticipated service non-availability shall be identified and analyzed
- Corrective actions shall be taken to address identified underlying causes for non-availability
- Changes to service availability requirements shall be reflected in the service availability plan

16.Budgeting and accounting Policy

The policy described to secure the appropriate funding to Sybrid to design, develop and deliver services that meet the strategy of the Sybrid ITS Tech Division and maintain a balance of supply and demand.

- Cost estimates shall be developed
- Results from cost estimates shall be used to produce budgets
- Deviations from the budget and costs shall be controlled
- Corrective actions shall be taken to resolve deviations from the budget
- Charging shall be implemented to recover the cost of IT provision, if applicable
- Deviations from the budget and costs shall be communicated to affected parties

17.Supplier Management Policy

Following is the supplier management policy of Sybrid at the Sybrid :

- Service Owners Shall ensure that externally provided processes, products and services do not adversely affect Sybrid's ability to consistently deliver conforming products and services to its customers.
- Every Supplier shall be evaluated for the product or service they deliver to Sybrid.
- Requirement shall be communicated to the suppliers in documented form, so it would have recorded and reproduced in the need.
- Sybrid abide by all applicable legal requirements and same expects from the suppliers, if any supplier is observed with the violating applicable legal activity shall be marked blacklisted and will not be contacted in the future.
- Sybrid reserves the right to conduct product or service verification or validation activity anytime, according to pre-agreed requirements.
- Formal information security risk assessment shall be conducted for all those suppliers with whom secret, confidential or private classified information needed to be shared.

18.Information Classification Policy

ITSM Steering team ensures protection of Data and Information residing with them based on their level of classification. It is further ensured that;

- Information, data and documents are classified according to their level of confidentiality, sensitivity, value and criticality for business activities, information security and client requirements
- Information is clearly labeled so that all users are aware of its classification
- Information is processed and stored strictly in accordance with the classification level assigned
- Classified information has an identified owner
- Authorized Personnel maintain and update a record of the information residing with them

19.Access Control Policy

Sybrid ensures restricted and effective Access Control system to prevent unauthorized access and unauthorized use by provision of;

- Access should be provided on a need-to-use basis and only when authorized.
- Sensitive and/or Confidential information should be accessed in accordance with the Information Classification, Labeling and handling Process.
- Requests for access to information and supporting assets should be adequately justified.
- A formal procedure should be followed for registering and deregistering users.
- Access Control Procedure should be followed for access authorization and review.
- Access rights should be reviewed on a regular interval. They should be modified/revoked whenever:
    - There is any change in a user's job assignments.
    - A user leaves the organization.
- Duties and area of responsibility should be segregated to increase accountability and to avoid the risk of accidental or deliberate system misuse.
- Authorization for access should be obtained from the information/asset owner.
- User accounts should not be re-issued to other persons and temporary user accounts should be deleted or deactivated when not required (or after the specified period).
- Formal records should be maintained of all registered users of a system.
- Privileged access rights for each system product e.g. operating system, database management system and each application should be identified along with the categories of employees to which they are allocated.
- System privileges should not be assigned to user accounts used for day-to-day activities.
- Password Management Policy should be followed.
- Users should only be able to access systems and/or network(s) for which they have been authorized.
- All users should have unique user IDs and should be authenticated using a password based two-factor authentication at least.

- System documentation and log files must be protected from unauthorized access.
- Access by external parties (e.g. customers, service providers etc.) if a business requirement arises should not be provided until the appropriate controls have been implemented and, where feasible, a contract has been signed that defines the terms and conditions for the connection or access.

20.Backup/ Retention & Restoration Policy

20.1. Purpose

The purpose of this policy is to set forth principles, procedures, and responsibilities for data backups, including the responsibility that users have regarding their own data.

Backup and recovery policy is to provide the continuity, restoration and recovery of critical data and systems in the event of an equipment failure, intentional destruction of data, or disaster.

20.2. Scope

The Sybrid ITS Tech Division requires that computer systems maintained by Information Services be backed up periodically, that the backup media be stored at a secure off-site location, and that recovery tests are performed on a regular basis. As a result, Information Services will adhere to information technology best practices which call for daily, weekly, monthly, and yearly system backups. This scheme allows systems to be restored with at most one working day data missing.

Information Technology Services department recognizes that the backup and restoration of data for applications are critical to the sustainability and operations of the respective departments. In order to maintain good quality of services, we ensure that Server's /data are backed up on a regular basis. The backup policy is divided into three terms.

The service and hence this policy has been designed and implemented with disaster recovery / business continuity (i.e. the ability to recover Server's / data in the event of a partial or total loss of Server's / data).

The 'Server's /Application data' backups cover all systems services managed by the IT department. Data held in local PC's is excluded from backup unless departments have specific arrangements with the IT department. All employees are responsible for their own PC or laptop's data backup by themselves. IT team have schedule backup of network drive for protection of data / support to sync your personal data to back up at Google drive.

Backups are NOT meant for the following purposes:

- Maintaining a versioned history of data.
- Personal data such as photos, videos, music, etc.
- Programs (i.e., applications) of any type (personal or officially supported)
- Exceptionally large images (scanned or digitized material) and large video files. If you need this type of storage space, please contact ITS to discuss alternative backup options.

20.3. Frequency

Incremental backups will be performed daily. Incremental backups will be saved for a full week. A full systems backup will be performed weekly. Weekly backups will be saved for a full month. The last weekly backup of the month will be marked as a monthly backup. Monthly backups will be saved for Six months. The last monthly backup of the year (June) will be marked as the yearly backup. Yearly backups will be saved for 3 years but financial backup retention will be according to FBR rule. Incremental, weekly, monthly, and yearly backup media that is no longer needed will be recycled or destroyed.

20.4. Backup

The saving of Server's / data to a backup storage media / tape drive / bank locker for the purpose of preventing loss of data in DC due to equipment failure or destruction.

20.5. Restore

The process of restore /recovery of Server's / data ensure that backup are restored from storage media / tape drive is according to defined RPO (recovery point objective) and RTO (recovery time objective).

20.6. Retention

Legal requirements or policies dictating records of specific types / data / Server be maintained in retrievable form for a specific period of time. Example: financial data backup must be retained for X years. Refer to the FBR_____.

21. Password Policy

21.1. Password Syntax and instructions

- Password syntax rules are as follows:
  - All user passwords must be at least 8 characters in length.
  - Passwords must contain characters from at least 3 of the following 4 categories:
    1. Upper-case alphabets (A-Z)
    2. Lower-case alphabets (a-z)
    3. Base 10 digits (0-9)
    4. Special characters (e.g. !, @, #, $, ^, &, etc.)
  - The maximum age of a password will be 90 days (i.e. a user cannot go more than 90 days without changing his/her password).
  - Password history will be maintained and users will not be allowed to repeat any of their 5 most recently used passwords.
  - A password cannot contain in entirety or a portion of the username
  - The account will be locked for 5 minutes after three unsuccessful attempts
- Passwords must not be disclosed to anyone. This includes employees, supervisors, managers or IT employees. If IT representatives need to access a user account in the user's absence, they will replace the password with a temporary password and this activity will be performed based on the Head of the Department's approval.
- A password cannot contain in entirety or a portion of the user name.
- Passwords should not be associated with anything personal related to users, their family or anything obvious that might allow the password to be guessed.
- Passwords should not be written down in an easily discovered location or format. A user should not enter a password if someone is watching, nor should a user watch other users enter their password.
- This policy in no way implies that any usage is private. The Company reserves the right to monitor all electronic data in accordance with this Information Security Policy and applicable laws.

- Providing any non-employee with access information, e.g., user login names and passwords is prohibited.
- Users are provided with approved login names to access the Company network and other electronic resources. Under no circumstances should an attempt be made to access the network with a login name or password other than that intended for the specific use of the person attempting such access.
- Unattended systems must not be left in a “logged in” state for periods in excess of fifteen minutes without a password protected screen saver. In anticipation of such periods, and especially when leaving the premises, users should either log out or lock the system.

21.2. Password Guidelines

In addition to the rules stated above, the following are a few don'ts to keep in mind when choosing passwords:

- Don't choose a password that is a dictionary word (English or foreign)
- Don't choose a password that is the name of a family member, pet or friend
- Don't choose keyboard, word or number sequences as passwords (e.g. 12345678, qwerty, asdfg, aaaaa, etc.)
- Don't choose passwords that are hybrids of the above
- Don't choose passwords that are any of the above spelled backwards
- Don't choose passwords that are any of the above followed or preceded by a digit (e.g. 1password, password1, etc.)
- Don't share passwords with anyone
- Don't insert passwords in emails
- Don't write down passwords in easily accessible places

A useful tip to consider when selecting a password is to base it on an easy to remember phrases. For example, the phrase might be "This may be one way to remember my password!" and the password could be: "Tmb1w2rmp!" or some other variation. Or the password can be a phrase itself; for instance, "aQuickBr0wnFox" or "SimpleP@$$word" or "BunnyRa66it", etc.

Important: Do not use any of the above examples as your passwords!

In case you have any queries regarding the new user password policy, please send an email to the following address: support@sybrid.com Sybrid ITS Tech Division.

Finally, thank you for your cooperation with regards to the implementation of this policy. This will be a vital step towards the provisioning of a secure and stable SYBRID ITS TECH DIVISION computer network.

22.Network Access & Internet Usage Policy (LAN or WLAN)

22.1. Definition

Term	Definition
Sybrid	All divisions, Departments and Campaigns, of the Karachi Sybrid ITS Tech Division
Employees	All full and part-time employees, and all temporary employees.
User	Any person accessing company networks and computers, all employees and any contract personnel having access to the Company's electronic systems.

22.2. Responsibility Matrix

User / Group	Responsibility
Head of Department – ITS	Monitors adherence to the policy by authorizing appropriate and regular checks on all Information Systems. Periodically modifies the policy to account for technological advances and legal developments.
IT Customer Support (Service Desk)	Communicate all the users regarding policy.
Networks	Network team will take care of issues and requests related to network connectivity (Wired LAN & Wireless LAN) for employees and guest of the Company.
All Users	All users must be familiar with the requirements of this policy and adhere to those requirements. In addition, they must report all breaches of this policy to the Service Desk.

22.3. Purpose

This policy serves as part of the management of network access and provision policy throughout the whole Sybrid.

This policy applies to:

- All those who are employees of Sybrid, permanent and temporary, visitors, vendors and contractors.

- All systems owned by the Sybrid or systems that are attached to Sybrid network either LAN or WLAN or systems having any kind of physical connectivity with Sybrid network.
- All assets/sources that required connectivity with the Sybrid network through any means. These sources include all electronic equipment, such as a printer, camera, biometric machines, multimedia's, laptop's, personal computers, mobiles and, tablets and etc.

22.4. Wired LAN – Network Access & Usage Policy

The local network is a facility that is to be used "responsibly" at all times by all members of the SYBRID. Hosting and transmitting material which is designed or likely to cause annoyance, inconvenience or needless anxiety to anyone is against usage norms, and will lead to action against individuals and groups involved in such activities.

22.4.1. Wired LAN access and usage policies

22.4.1.1. Access

The users reside inside Company data network can only be connected with the organization's network, provided they are going to use the Sybrid's/personal workstation. In case the network node (connection) is available in the vicinity of the user, he/she will use this connection with the help of patch cord.

If there is no node (connection) available, as well as in case if available node (connection) is faulty please log your ticket to help desk.

22.4.1.2. Usage

The Sybrid data network extends to all Sybrid floor. Use of the internet by users of SYBRID ITS TECH DIVISION is permitted and encouraged where such use supports the goals and objectives of the business. However, SYBRID ITS TECH DIVISION has a policy for the use of the internet whereby users must ensure that they:

- Comply with current legislation
- Use the internet in an acceptable way

- Do not create unnecessary business risk to the company by their misuse of the internet.

22.4.1.3. Unacceptable behavior

In particular, the following is deemed unacceptable use or behavior by employees:

- Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material.
- Using the computer to perpetrate any form of fraud, or software, film or music piracy.
- Using the internet to send offensive or harassing material to other users.
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such license.
- Hacking into unauthorized areas.
- Publishing defamatory and/or knowingly false material about [business name], your colleagues and/or our customers on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format.
- Revealing confidential information about [business name] in a personal online posting, upload or transmission - including financial information and information relating to our customers, business plans, policies, employees and/or internal discussions.
- Undertaking deliberate activities that waste employees effort or networked resources.
- Introducing any form of malicious software into the corporate network.

22.4.1.4. Company-owned information held on third-party websites

- If you produce, collect and/or process business-related information in the course of your work, the information remains the property of SYBRID ITS TECH DIVISION. This includes such information stored on third-party websites such as webmail service providers and social networking sites, such as Facebook and LinkedIn.

22.4.1.5. Monitoring

- SYBRID ITS TECH DIVISION accepts that the use of the internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business.
- In addition, all of the company's internet-related resources are provided for business purposes. Therefore, the company maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

22.5. Wireless LAN Network Access & Usage Policy

Information Technology has a commitment to provide ubiquitous wireless coverage as possible in organization space within resource constraints and priorities. Priorities for the installation and maintenance of wireless spaces will be determined by the network team in consultation with other Sybrid administrators utilizing the following criteria:

- The population density frequenting a Sybrid space, public service areas that are visited by relatively large groups of users will have top priority.

Information Technology (IT) a division of Information Technology, shall act as the central management authority in regulating the installation, maintenance and ongoing management of all wireless LAN systems used by BUs, as well as spectrum management within the borders of company or any remote location/office directly connected to the Sybrid network.

22.5.1. Requirements

- All end-user devices or systems connecting to the enterprise network infrastructure must comply with the same policies, procedures, and practices governing the use and operation of any end user device or system connecting to the Sybrid wired network.
- No Wireless LAN may be placed into operation without advance consultation and registration with IT.
- All Wireless LANs will be operated in such a manner that they do not interfere with other WLANs or the Sybrid enterprise wired data network

- All wireless network access shall utilize the enterprise authentication, authorization and encryption mechanisms prescribed by Information Technology.

22.5.2. Departmental Responsibilities

- Departments shall request installation, repair, replacement or the move of an existing access point from IT.
- Department shall be responsible for all costs associated with installation, repair or replacement of its access points.

22.5.3. ITS Responsibilities

- IT is responsible for establishing and maintaining standards for wireless access points (equipment and installation) for use at the Sybrid ITS Tech Division.
- All Wireless LAN systems shall be installed, configured and managed by IT.
- IT will maintain a database of access points, their locations, the frequencies in use, the circuit numbers connecting the access points to the Sybrid's Network, and the name(s) of the department's designated Technical Liaison.
- IT will attempt to resolve frequency coordination problems between Wireless LAN owners. However, IT cannot guarantee interference-free operation of any WLAN from other unknown or non-company Wireless LAN (WLAN) systems or from other devices operating in the same spectrum as the WLAN.

22.6. General Wireless LAN Policy

- Personal Wireless Access Points/Wireless Routers, called Rogue Access Points (RAPs), are not allowed to be installed on Sybrid by any employee because they disrupt the wireless services provided by SYBRID ITS TECH DIVISION Wireless LAN.
- Anyone found installing personal Wireless Access Points (APs)/Wireless Routers anywhere in the Sybrid will be subjected to appropriate disciplinary action and the device(s) will be confiscated.
- Anyone who needs to deploy Wireless Access Points/Routers to fulfil any business requirement must inform and get approval from ITS in writing. ITS will approve the

use of these devices for a specific period of time, after which approval will need to be re-sought.

- Anyone found manipulating WLAN devices will be subjected to disciplinary action; the actions include moving the antennas direction, relocating APs or manipulating AP power.

22.7. Executive WLAN Policy

Total unrestricted access has been provided to executives and top management. The worthy Head of Department will provide the approval for executive access, which is being controlled on the basis of device's mac address. This access is provided both on laptop and Cell phone.

22.8. Management WLAN Policy

Every management member is allowed to have WLAN access on laptop or Wi-Fi enabled desktop to connect, users will provide mac address to ITS to avail the facility. Social media access is prohibited for management.

22.9. Employee WLAN Policy

Laptop users are allowed to have WLAN access on laptop, user will provide mac address to ITS to avail the facility. Social media access is prohibited for employees except HODs approval.

22.10. Event WLAN Policy

Internet access is provided to users for seminars or events conducted at Sybrid ITS Tech Division. The customer (admin/HoD) has to inform ITS 1-week prior the event to avail the facility. ITS will arrange the internet facility for event/seminar as per requirement.

22.11. Guest WLAN Policy

Internet access is to be provided to the guests of Sybrid ITS Tech Division., the guest always connects to Guest account to get the Sybrid ITS Tech Division-guest password, which always get changed after the week.

22.12. Visitor WLAN Policy

Internet access is to be provided to the guests of Sybrid ITS Tech Division, every concern person contacts servicedesk if required internet access for his guest who coordinates with network team and enables the Wifi access for guest, the password get changed after the week.

22.13. Hotspot Usage Policy

Hotspot is strictly prohibited in the Sybrid ITS Tech Division network.

22.14. Internet Usage Policy

Our internet usage policy outlines our guidelines for using our company's internet connection. We want to avoid inappropriate or illegal internet use that creates risks for our company's legality and reputation.

The tables show the categories who are allowed to use internet under these access and protection levels.

22.14.1. Access Level

Access Level	Description
AL1	Any (Full Access)
AL2	Social Media, Streaming Media, Youtube, Communication Media, Normal Browsing
AL3	Normal Browsing, WhatsApp, Skype
AL4	Conditional Access
AL5	Conditional Access time based

22.14.2. Protection Level

Protection Level	Description
PL1	IPS, AMP, Adware/Malware Sites, APP Firewalling, URL Filtering
PL2	IPS, Adware/Malware Sites, APP Firewalling, URL Filtering
PL3	APP Firewalling
PL4	No restriction

22.14.3. Categories for Internet Usage

Sr.	Category	Roles / Designation	Devices	Protection Level	Access Level	Approval Required	Approving Body
1	Executive's & Top Management	CEO, CSO and HODs	Any	PL1	AL1	Yes	-
2	Management	Managers, AMs, Supervisors and TLs	Laptop/ Desktop	PL1	AL3	No	Respective HOD
			Mobile Devices	PL1	AL3	Yes	Respective HOD
3	Guests	All SYBRID ITS TECH DIVISION guests in Guest House	Any	PL1	AL5	Yes	Respective HOD
4	Visitors	All approved visitors	Any	PL1	AL5	Yes	Respective HOD

23. Network Infrastructure Deployment Policy

23.1. Existing Infrastructure

Whenever required for addition / removal in existing infrastructure related to the followings:

- Network point
- Access point
- Switch

23.1.1. Customer/Requester Responsibilities

- Submit the ticket for network access (LAN/WLAN) for one or more users
- Customer will provide the approval to activate the infrastructure in case cost is involved.
- Get the approval on BOQ from competent authority.

23.1.2. ITS Responsibilities

- ITS Networks team will review and assess the customer requirements.
- Network Team will activate or deploy new data point if infrastructure is available and cost is not involved.
- ITS Networks team will prepare the BOQ, which needs to be approved by the competent authority when cost involved.
- ITS Networks team will share the details with ITS Management for new requirements after approvals
- ITS Management review and approve the requirements for further execution.
- ITS Networks team will execute the task related to addition of network points / access points / switches.

23.2. New Infrastructure

Whenever needs to deploy network infrastructure related to the newly addition of Building, Floor etc.

23.2.1. Customer/Requester Responsibilities

- Share the requirements for new network infrastructure
- Share the layout plans with the ITS team
- Get the approval on BOQ from competent authority
- Work for PO with concern teams related to the requirements
- Make sure for clearance of the payments related to PO.

23.2.2. ITS Responsibilities

- ITS team will review and assess the customer requirements
- ITS Networks team will get the BOQ reviewed and approved by the network department HOD
- ITS Networks team will provide the BOQ to customer/requester for approval
- ITS Networks team will share the BOQ with ITS Management for new requirements
- ITS Management will review and approve the requirements for sharing with customers.
- After approval network team will forward BOQ to Respective team, who will engage the vendor to perform the said task and arrange required equipment.
- ITS Networks team will coordinate with assigned vendor until the completion of the project.
- Network team will configure the network devices, which will be deployed by vendor.
- Network Team will perform inspection after completion, afterwards SPMO will proceed for the payment.

23.3. Special Situations/Exceptions

No Exceptions and in all the cases will have to follow the policy by both parties (ITS and customers).