PIT-201

Information Technology Process

Revision / Version	Date	Comments
1.0	08/10/2008	Nil
1.1	01/05/2009	Nil
2.0	30/11/2009	Nil
3.0	01/01/2013	Nil
3.1	16/07/2013	Nil
3.2	22/10/2013	Clause 3.6 / Associated Records Updated
3.3	05/12/2013	Addition of forms
4.0	14/05/2015	Addition of software management requirement
5.0	15/03/2016	Process Revamping
6.0	17/03/2017	Addition of Types of Changes
6.1	1/03/2018	Removal process & form of Change Management

Table of Content

1. Purpose:

The purpose of this document is to describe the Information Security, Network, Systems, Voice Infrastructure and Computer operating procedures for SYBRID. It will describe the business requirements for Network, Systems, Voice Infrastructure and support. Roles and Responsibilities at different level are also identified in the document. Communication channels for assistance are also elaborated.

Operating procedures for Anti Malicious and Mobile Code, User Account Management, Security Management, Management of Removable Computer Media and Security Configuration Guide for Operating System and Software will also be enclosed in this document.

2. Scope:

The requirements of this procedure apply to all IT processes to meet the compliances of ISMS to regulate a hi-tech and fully controlled environment for IT service delivery with the following practices.

- I.T. Services Operations Management.
- Configuration Management.
- Change Management.
- Asset Management.
- Access Rights Management.
- Information Security Management.
- Capacity Management.
- Project Management.
- IT Disaster Recovery & Business Continuity Procedure

3. Definitions:

Abbreviations/Terms	Description
IP	Internet Protocol
FTP	File Transfer protocol
LAN	Local Area Network
ISP	Internet Service Provider
SLA	Service Level Agreement
OLA	Operational Level Agreement
BU	Business Unit
CS	Customer Services
MD	Medical Division
TS	Telecom Services
BD	Business Development

NMS	Network Management System
UAN	Universal Access Number
TFN	Toll Free Number

4. Processes and Policies:

- Sybrid IT Team must be provided legitimate training regarding the Policies, procedures, running systems, services and information security compliances at the time of hiring. These records will be maintained in **RIT-224 IT Resource Training Record.**
- Access to any required information to any Sybrid IT Team member must be on the basis of completion of training.
- Manager/A.M. IT must ensure that initial training is completed and successful prior to setting up the particular IT resource operational in LIVE environment.

4.1. I.T. Services Operations Management

Sybrid IT Team is responsible to provide all the IT enabled services and responsible to provide these services with a combination of in house and third party services to meet the business requirements for internal and external customers. Following IT Services will be included in scope of work.

- Networks Services
- Telephony Services
- Internal Network
- Infrastructure & Applications Services
- Service Desk

4.1.1. Call Logging and Escalation Process

All the incidents, problems, service requests and queries will be logged into **Sybrid IT Service desk (**http://servicedesk.int.sybrid.com **for KHI or** http://helpdesk.sybts.local/ **for ISB**) as per the following procedure.

- Customer will report all its tickets to IT Support via **Sybrid IT Service desk** or Email (support@sybrid.com/Support@sybridts.com) or by calling 3000/6004 extension.
- System Support Engineer will log ticket complaint in **Sybrid IT Ticketing system** and the ticketing system generates a unique ticket ID that captures the event, event source, initial event severity and event Priority
- IT Department uses this unique ticket ID for formal communication with customer as a reference number.
- System Support Engineer will try to resolve it over the phone, if not able to resolve he/she will visit the individual on his/her seat.
- System Support Engineer will escalate this issue to Systems Engineer/Administrator if any

backend configuration changes are required.

- Systems Engineer will resolve it by making changes on backend configuration. If he is unable to resolve it and requires some major configuration change he/she will escalate it to Systems Administrator.
- If Systems Administrator is unable to resolve and requires some strategic/Design level change he will escalate it to AM-IT/ Manager IT.
- System Support Engineer will update the ticket on **Sybrid IT Service desk**
- **Sybrid IT Service desk** Ticket will also be updated by Support engineer even if the problem is resolved over the phone and ticket will be closed after client approval through helpdesk.
- System, Network and Voice Support Engineers are available in all shifts and will respond to all the emails on **support@sybrid.com/Support@sybridts.com** and calls on extension 3000/6004.
- In case of any escalation is required he will perform it as per defined process.
- IT Team Lead will ensure that all emails and extension calls are entertained properly as per agreed SLA/OLA.

4.1.2. Service Provider, Vendor and Partner Escalation

Sybrid IT will perform escalation to service providers, vendors and partners for third party services in case if required as per the following details.

In case of any Service Downtime, it must be calculated on the basis of **RIT-209 IT Uptime Report** and a rebate shall be claimed to the service provider as per rebate criteria mentioned in Contract.

Service	Service Provider	Method	Email
Internet/ Data Connectivity	Cyber Internet Services	* By Calling CN NOC 5654 * Email on provided addresses	helpdesk@cyber.net.pk noc_khi@cyber.net.pk tac-south@Cyber.net.pk
Telephony Services CS & TS - (UPL, Haier, OPTP, CAP, IMC & Interwood)	Multinet	* By Calling MN NOC 111 247 000 * Email on provided addresses	ots@multinet.com.pk fll.noc@multinet.com.pk inam.haider@multinet.com.pk
Telephony Systems & Services CS - MCD, Colgate and 'CYBERNET)	Cyber Internet Services	* By Calling CN NOC 5940 * Email on provided addresses	ngn-noc@cyber.net.pk

Telephony Services MD (Back Office, Front Office)	InPhonex	*Open a ticket on InPhonex Portal	www.inphonex.com
Telephony Services MD (Systec)	Alcazar Network	*Email on provided address	support@alcazartnetworks.com
Sybrid Karachi PBX-External	Cyber Internet Services	* By Calling CN NOC 5940 * Email on provided addresses	ngn-noc@cyber.net.pk
Sybrid Islamabad Internet Service	Multinet Private Limited	* By Calling MN NOC 111 247 000 * Email on provided addresses	OTS@multinet.com.pk fll.noc@multinet.com support@multinet.com
Sybrid Islamabad Internet Service	NayaTel Internet Services	* By Calling NT NOC 111 114 444 * Email on provided addresses	support@nayatel.com

4.1.3. Incident Management

- Services downtime or serious performance degradation and information security risk/breach shall be considered as an Incident and shall be managed according to incident classification in terms of its severity and impact on IT operations in line with the Incident Reporting and Response Procedures.
- Incidents affecting service impact and security shall be reported through appropriate escalation process to Sybrid IT (Refer to IT Call logging & Escalation process).
- Root Cause Analysis will be carried out for every incident which provides a substantial service impact and security risk.
- An incident report shall be created; types, volume and costs of the incidents and malfunctions to be quantified and monitored and maintained in **RIT-203 Service Incident Report** and share it with relevant stake holders with in next 24 hours.
- Any security incident or weakness must be maintained on **RISM-902** by following the Security incident/weakness reporting procedure.

4.1.4. Problem Management

- Re-occurrence of incidents on similar pattern will be considered in Problem Management.
- Root Cause Analysis will be carried out for every problem which provides a substantial business impact.
- Sybrid IT Team will explore best possible solution and perform rectification in order to give the permanent fix to problems.
- All the trends and reporting shall be maintained on Sybrid IT Service desk
- Sybrid IT will ensure all the problems are managed as per agreed SLAs/OLAs.
- After the problems are resolved System Support Engineer will close the ticket at helpdesk system.

4.1.5. System Health Check and Audit

- System, Network or VoIP Support Engineers are responsible to perform weekly health check and Audit to review system performance and logs.
- If System, Network or VoIP Support Engineers found any unwanted or personal data on shared system, software, malware or any malicious content on employee's system incident should be raised by following security incident & weakness reporting mechanism.
- All the system audit checks will be maintained in **RIT-213 System Audit Report**.
- All the System health checks will be maintained in **RIT-212 System Health Check Report**.

4.1.6. Server Maintenance

- System, Network or VoIP Engineers are responsible to perform bi-monthly maintenance and review system performance and event logs of servers.
- Maintenance will always be planned and informed to senior Management at least before 24 hours. This intimation will be circulated through notification on ERP Portal.
- In case of any urgent maintenance IT Team will inform all HODs via notification on ERP Portal just before the activity.
- Any vulnerability observed shall be noted and highlighted to the concerns prior to performing any corrective actions.
- All the system maintenance activity will be updated in **RIT-211 Maintenance Report**.

4.1.7. Network Resources Monitoring

- System, Networks or VoIP Support Engineers are responsible to monitor Network resources (Bandwidth, Broadcast, Port Utilization and other traffic) using Solar winds NMS. (http://192.168.61.198/Orion/Login.aspx for KHI & http://isb-nms-d001/Orion/Login.aspx for ISB) with their provided credentials by using **GIT-204 Client end Configuration** for Karachi & **GIT-304 Client End Configuration Guideline-ISB** for Islamabad site.
- Specified thresholds (75%) are defined for respective services and devices in monitoring system and in case of its breach some alarms are generated.
- In case of any alarm is generated System, Networks or VoIP Support Engineer will highlight it to Systems Engineer and Systems, Networks or VoIP Administrator for further diagnosis & troubleshooting.
- Any unusual activity over internet will be reported to specific line manager and ISM for further disciplinary action.
- In case any unusual behavior of any service or device is observed, Systems Engineer will notify all stakeholders and perform required maintenance.
- Daily Monitoring activity will be updated in **RIT-222 Daily Network Monitoring Sheet** by System, Networks or VoIP Support Engineer and will be updated on ERP portal at day end.

4.1.8. Servers Resources Monitoring

- System, Networks or VoIP Support Engineers are responsible to monitor Server resources (RAM, CPU, Storage, Network and Power utilization) using VMware Server Monitoring for Karachi servers refer **GIT-204 Client end Configuration** and **GIT-304 Client End Configuration Guideline-ISB** for Islamabad servers with their provided credentials.
- Specified thresholds (75%) are defined for respective services and devices in monitoring system and in case of its breach some alarms are generated.
- In case of any alarm is generated System Support Engineer will highlight it to Systems, Networks or VoIP Engineer/Administrator for further diagnosis and troubleshooting.
- Any unusual activity with data held on servers will be reported to specific line manager and QA for further disciplinary action.
- In case any unusual behavior of any service or device is observed, Systems Engineer will notify all stakeholders and perform required maintenance.
- Daily Monitoring activity will be updated in **RIT-223 Daily Server Monitoring Sheet** by System, Networks or VoIP Support Engineer and will be updated on ERP portal at day end.

4.1.9. Telephony Services Monitoring

- System, Networks or VoIP Support Engineers are responsible to monitor Telephony Services by testing UAN/TFN and backend numbers.
- Any vulnerability observed should be immediately highlighted to concerned service provider/service owner for resolution.
- In case any unusual behavior of any service or device is observed, Systems Engineer will notify all stakeholders and perform required maintenance.
- Daily Monitoring activity will be updated in **RIT-221 Daily UAN Audit Sheet** by System, Networks or VoIP Support Engineer and will be updated on ERP portal at day end.

4.1.10. Daily I.T. Checklists

- System, Networks or VoIP Support Engineers are responsible to perform daily floor checklist prior to shift start.
- Daily Floor checklist shall be updated on ERP Portal **RIT-225 Daily IT Floor Checklist-Sybrid MD**, **RIT-226 Daily IT Floor Checklist-Sybrid CS** and **RIT-229 Daily IT Floor Checklist-Sybrid TS.**
- Systems Engineers/Administrators are responsible to perform daily servers, networks and telephony checklists.
- In case any unusual behavior of any service or device is observed, Systems Engineer/Administrator will notify all stakeholders and perform required maintenance.

4.1.11. I.T. Roster Management

- Sybrid IT plan roster for IT Team according to work load with 24/7 availability.
- On Weekdays (Monday to Friday) all engineers were available according to their shifts for Karachi IT Team whereas for Sybrid Islamabad roster will be managed for all seven days with 1 off day for every engineer on any day of the week..
- On weekend (Saturday & Sunday) 1 off for all engineers according to roster.
- Sybrid IT Roster is formed monthly by Team Lead and reviewed by Manager I.T. and A.M. I.T. which is shared to all stake holders via email.

4.1.12. I.T. Service Provider/ Vendor Management

- Sybrid IT team must ensure proper screening of Vendors/ Service providers and partners considering the Type of services meeting the business requirements, Cost of services, Quality of Services & information security risk.
- Sybrid IT Team must ensure SLA with the service provider to ensure all the necessary business and information security requirements.
- Any SLA between Sybrid IT and service provider must include the following points.
  - Service Provider Call Logging process & Escalation Matrix with TAT.
  - Mutually agreed pricing, billing and rebate structure.
  - Dispute resolution between two parties.
  - Information Security & Access to information.

4.2. Configuration Management

Configuration Management shall be carried out by IT in consideration for three of the below categories.

- Services Configuration.
- Server, Network and VoIP Systems Configuration.
- End-User configuration.

4.2.1. Services Configuration

- Manager / Assistant Manager I.T. shall be responsible to carry out selection of service provider to perform service configuration after appropriate evaluation.
- Manager / Assistant Manager I.T. shall engage required resources from Sybrid IT team to perform service configuration.
- Manager / Assistant Manager I.T. will ensure appropriate SLAs for third party services.

4.2.2. Server, Network and VoIP Systems Configuration

Systems, Network or VoIP Engineers shall be responsible to carry out the entire configuration on the following devices with the assistance of Systems, Network and VoIP Administrators.

- Application/Database Servers.
- VoIP Servers.
- Infrastructure Servers.
- Proxy Servers.
- Active Directory Servers.
- File Servers/FTPs.
- Email Servers.
- Access Switches.
- IP Phones.
- Wireless Access Points.
- Network Printer/Scanner.
- Multimedia Devices.

Systems, Network or VoIP Administrator shall be responsible to carry out the entire configuration on the following devices with the assistance of Manager I.T/ Assistant Manager I.T.

- Application/Database Servers.
- VoIP Servers.
- Infrastructure Servers.
- Proxy Servers.
- Active Directory Servers.
- File Servers/FTPs.
- Email Servers.
- Backup Servers.
- Access Switches.
- IP Phones.
- Wireless Access Points.
- Routers.
- Core & Distribution Switches.
- Perimeter, Edge or Data Center Firewalls.

All the configuration of above mentioned devices shall be incorporated in Configuration Management document **GIT-201 Infrastructure Configuration Management Guideline** for Karachi and **GIT-301 Infrastructure Configuration Management Guideline-ISB** for Islamabad after reviewed by Manager IT.
Any change in configuration shall be performed according to **Change Management Process**.

4.2.3. End-User Configuration

Systems Support Engineer shall be responsible to carry out the entire following configuration at end user refer **GIT-204 Client End Configuration**. He will take assistance from Team Lead-

Support or System Engineer in case it is required.

- Desktop Installation/Configuration
- IP Configuration
- Software Installation/Configuration.
- Printer Configuration.
- Soft Phone Configuration.
- Email (Outlook) Configuration.
- Hardware Configuration.
- Multimedia Configuration.
- Service (Internet, VPN etc.) Configuration.

Systems Support Engineer shall be responsible to install/configure any software as defined in **RIT-217 Approved Software list**.

IT department will be responsible to update approved software list while considering operational requirement with the help of Need Analysis and considering all licensing agreement, legal & statutory requirement.

Any services or hardware access will be configured according to the access rights management process.

All the configuration of client end will be incorporated in **GIT-204 Client End Configuration for Karachi** and **GIT-304 for Islamabad.**

4.3. Change Management

4.3.1. Change Management Obligation

Change management will be implied according to **PISM - 907 Change Management Process**

4.3.2. Change Management Request for Movement of Fixed Assets

Change management will be implied according to **PISM - 907 Change Management Process**

4.3.3. Change Management Review

- Any Change will be reviewed on a monthly basis sequentially on data share as mentioned in the change management report/form for a specific area in a cycle to ensure review of all changes.
- After the review completion, change management report will be forwarded to ISM for verification.

4.4. Asset Management

4.4.1. I.T. Acquisition / Requisition Process

- Departments identify the need for acquisition/requisition of a product through the relevant manager using **RAD-403 Stock issuance & purchase requisition** for Karachi &

RIT-202 IT Requisition form for Islamabad.

- Users will also initiate request on I.T. Ticketing System.
- The relevant line manager is responsible for assessing the need for the required product and forwarding it to the IT Manager.
- IT Manager will perform need assessment and approve/disapprove on need basis.
- Sybrid IT will check if any existing inventory can be accommodated to fulfill the need in this case.
- IT Team with IT Managers approval is responsible for technical assessment of the purchase requisition.
- IT Team with IT Managers approval forward the requisition with complete specification details to Admin department.
- IT Team forwards the requisition with quotation and CEF or Expenditure form to the initiator of the requisition for budget confirmation/approval as per finance approval matrix.
- After receiving approved CEF or Expenditure, Sybrid IT submits the requisition to Admin Department.
- Administration verifies the approval and initiates PO for vendor.
- Products are received and checked by IT Team according to **RAD 403 for KHI or RIT-202** for ISB.
- Finance will paste a tag on the product and System Support Engineer will update inventory on asset inventory sheet.
- Initiator receives the resolution email from system, and confirms the completion of the request, and close the ticket on Complaint Management System If user is not satisfied then the ticket will be re-assigned to IT Support Executive.

4.4.2. Equipment Issuance

- Departments identify the need for replacement of a product through the relevant supervisor using **RAD-403 Stock issuance & purchase requisition** for Karachi & **RIT-202.**
- The relevant line Manager is responsible for assessing the need for the required product.
- Request will be forwarded to Manager/AM IT by sending **RAD-403 Stock issuance & purchase requisition** for Karachi & **RIT-202 IT Requisition form** for Islamabad.
- IT Team will issue the inventory according to the request in **RAD-403 Stock issuance & purchase requisition** for Karachi & **RIT-202 IT Requisition form** for Islamabad.
- IT Team will deliver the required products as per the request of end user.

4.4.3. I.T. Inventory Management

- Sybrid IT Team will maintain asset inventory on ERP portal.
- Sybrid IT will maintain its backup inventory on **RIT-205 Backup Inventory** for all the desktops, laptops, head gears and LCDs.
- Sybrid IT will maintain Data Center equipment inventory on **RIT-205 Backup Inventory** for all servers, switches, routers and other equipment's.
- Sybrid IT Asset inventory will be reviewed by Manager/A.M. I.T.

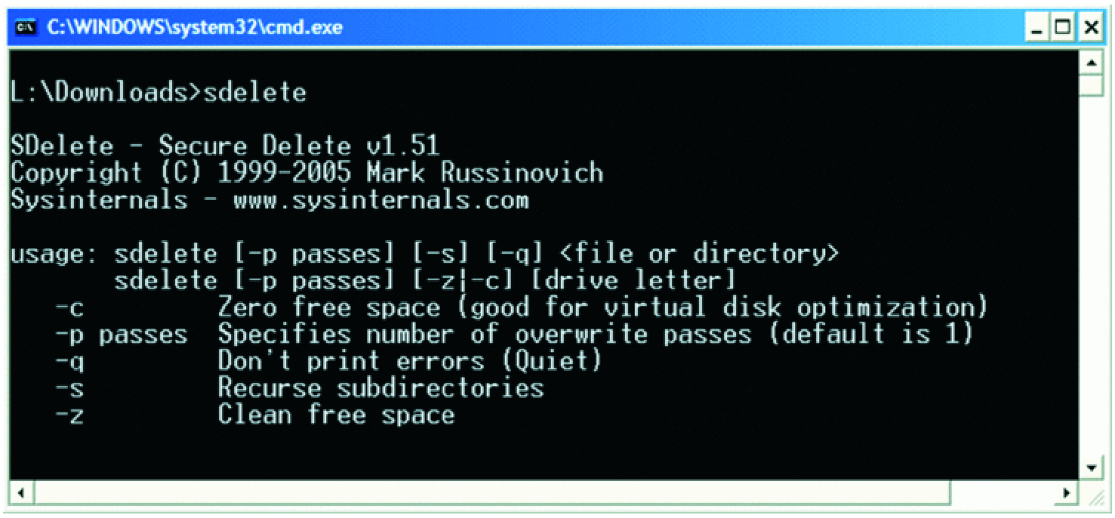
4.4.4. Secure Disposal and Reuse of I.T Equipment

It includes the process; regarding steps to be taken by I.T support executives for reuse and disposal of I.T equipment.

I. <u>Reuse:</u>

For reuse of storage media, I.T support executives will use “SDELETE” (File Shredder Software) utility to clean the media. Before assigning it to any employee, Steps for using SDELETE are mentioned below:

- sdelete [-p passes] [-s] [-q] <file or directory> , sdelete [-p passes] [-z|-c] [drive letter]
- -c (Zero free space (good for virtual disk optimization)).
- -p passes (Specifies the number of overwrite passes (default is 1))
- -q (Don't print errors)
- -s (Recurse subdirectories [Note: The contents of all subdirectories are included in the deletion or disk wipe.])
- -z (Cleans free space [Note: this is similar to the -c option except -z uses a random string of values to more securely wipe free disk space.])



```
L:\Downloads>sdelete

SDelete - Secure Delete v1.51
Copyright (C) 1999-2005 Mark Russinovich
Sysinternals - www.sysinternals.com

usage: sdelete [-p passes] [-s] [-q] <file or directory>
       sdelete [-p passes] [-z|-c] [drive letter]
   -c         Zero free space (good for virtual disk optimization)
   -p passes  Specifies number of overwrite passes (default is 1)
   -q         Don't print errors (Quiet)
   -s         Recurse subdirectories
   -z         Clean free space
```

II. <u>Secure Disposal:</u>

If I.T support executive found any equipment to be dead or no possibility of its reuse is found then secure disposal of equipment will be necessary. Below are the steps for secure disposal:

- I.T support executive will check for any possibility; if equipment can be reused.
- If the equipment is reusable then above mentioned process of Reuse will be followed.
- If I.T support executive found equipment to be dead then it will be provided to Administration Department.
- Upon receiving the equipment from I.T, admin will break the storage into pieces so that it can be shred securely.
- I.T will then modify its asset inventory accordingly and update these equipment details in **RIT-231 Disposal List**.

4.5. Access Rights Management

Access rights management will be performed according to **ISMP-902 Access control policy**. Regarding the I.T.'s domain it involves following access types controlled by Sybrid IT.

- ○ Internet Access
- ○ Internal Network Access
- ○ Printer/Scanner
- ○ File Server/FTP Access

- Any request must be reviewed and approved by respective reporting authority prior to access granting.
- Access can be of two type "Temporary" or "Permanent", temporary access will be revoked on completion of provided date and permanent access will be revoked on termination of services of an employee.
- Any request must be reviewed and approved by Sybrid IT prior to access granting while considering need analysis, all kinds of risks and ripple effects.
- Sybrid IT and C&A has right to disapprove any request considering the need analysis, risks and chances of data theft or security leakage.
- User must define the following information while generating this request.
  - ○ Access Type: Read, Read & Write, Application or Website
  - ○ Resource Name: (Name of resource on which access is required)
  - ○ Justification: (Business requirement for this access type)
  - ○ Required access from: (Date from which access is required)
  - ○ Required access till: (Date till which access is required)

4.5.1. Internet/ Wireless Access

- ▪ Any Internet resource (Website, Wireless, VPN etc.) access request shall be generated by Sybrid employee via Sybrid Workflow erp.sybrid.com/Workflow/Access Rights on ERP Portal for Karachi where as he/she will fill **RIT-214 Access Rights Form** for Islamabad.
- ▪ After all approvals support engineer saves the WIFI password and assign an IP to the device himself from centralized IP sheet and then update the IP sheet accordingly.
- ▪ System Engineer will grant any approved access to the internet from proxy servers.
- ▪ In case there is a change in any access policy defined at proxy server it will be done according to change management.

4.5.2. Internal Network

Any Internal Network resource access request shall be generated by Sybrid employee via Sybrid Workflow on ERP Portal erp.sybrid.com/Workflow/Access Rights for Karachi where as he/she will fill **RIT-214 Access Rights Form** for Islamabad.

4.5.3. Printer/Scanner

Any Data resource access request shall be generated by Sybrid employee via Sybrid Workflow on ERP Portal for Karachi where as he/she will fill **RIT-214 Access Rights Form** for Islamabad.

- Support engineer will provide printer/scanner access after all approvals as defined in **GIT-204 Client End Configuration**

4.5.4. File Server Access

Any File Server resource access request shall be generated by Sybrid employee via Sybrid Workflow on ERP Portal for Karachi where as he/she will fill **RIT-214 Access Rights Form** for Islamabad.

- System Engineer will provide any access after all approvals on Data/Folder which shall be followed according to **GIT-202 Data Management Guideline** for Karachi and **GIT-302 Data Management Guideline-ISB**

4.6. Access Rights Review

- Access Rights will be reviewed on a monthly basis sequentially on data share as mentioned in the review access right report for a specific area in a cycle to ensure review of all access rights by using this link http://erp.sybrid.com/Access right review report only for Karachi site.
- Manager/AM IT will review all the rights of internal network, servers, administrator access of servers using server audit software (for Microsoft servers) whereas for linux servers it will be reviewed from its default user lists.
- Manager/AM IT will review all the rights of Internet access from proxy servers.
- QA have the rights to review all the access requests which were being granted to users.
- For Islamabad Site all the access rights will be reviewed with the record document **RIT-215 Review Access rights Form.**

4.7. Information Security Management

- All the configuration details of every parameter regarding below mentioned procedures will be applied according to **GIT-201 Infrastructure Configuration Management Guideline & GIT-301 Infrastructure Configuration Management Guideline-ISB** for Karachi and Islamabad respectively.
- Any unauthorized person does not have access to these resources; any login attempt shall be denied.
- Sybrid IT must ensure that no user has rights to install any software, utilities, patches, drivers or any kind of application unless there is a severe business need which is justified and meeting the information security requirements.
- The privileged access rights are prohibited in Sybrid, but the allocations of these rights are given after formal approval from the top management via email and using the same process.
- Sybrid IT must ensure that no user has rights to install any software, utilities, patches, drivers or any kind of application unless there is a severe business need which is justified

and meeting the information security requirements.

- All the privilege access users will be listed in **RIT-230 Privilege access user list** along with the details of their privileged access and authorities. These details will be shared with ISM on quarterly basis.
- Any privileged user access rights will be reviewed by Manager IT /A.M. IT on quarterly basis and Manager IT/AM IT rights will be reviewed by ISM.

4.7.1. Event Logging

Types of logs being reviewed;

- Active directory log.
- Proxy server logs.
- Microsoft Exchange Server Logs.
- VoIP Server Logs.

Authorized personnel who have rights to view and export logs;

- Manager/A.M. I.T.
- Systems Engineer/Administrator

People authorized to log extraction and review request;

- IS Manager
- Manager/ A.M. I.T.

System Engineer/Administrator logs will be reviewed by Manager/AM IT & Manager/AM IT logs shall be reviewed by ISM on monthly basis.

These Logs for Microsoft Servers will be reviewed by server audit software whereas for linux servers it will be reviewed by its default feature.

4.7.2. Network Security & Management

In order to networks with segregated environment for end-users, servers and devices we have got:

i. Separate VLANs implemented for:
  a. Network device management.
  b. End-user traffic separation from the server network.
  c. Server traffic separation from the end-user network.

ii. Server network protection from direct access from the internet via a PERIMETER Network firewall.

iii. Wireless network implementation of WPA2-PSK.

iv. Sybrid IT must ensure that no user has access to change any Network Privileges.

4.7.3. Email Transmission

Employee will have a limited access of sending and receiving of emails, employee can only send/receive emails at sybrid.com/sybridmd.com/sybridts.com exchange domains. Email access will be extended with due justification of business needs considering the security impacts.

4.7.3.1. Encrypted Emails

All emails that contain either Text / Attachments would be sending via controlled Google Email Services and Microsoft Exchange Server with encrypted emails.

4.7.3.2. Authorized access

Sybrid IT will provide authorized restricted access of emails for each employee at the request of employee's line manager mentioning in new starter form.

4.7.3.3. Access Levels

Sybrid IT will provide following mentioned email access on the basis of request these accesses includes

- Local Email Access
- External Emails Access (Inbound/Outbound)

4.7.4. User Account Management

SYBRID associates will require a unique id to access SYBRID domain Server, network, corporate applications, SharePoint portal, Servers and applications. This ID will be created on our AD server at the time employee joins organization. User account management will be the responsibility of systems engineer.

- Every associate in SYBRID have a unique login identity.
- For a new hire id request will be generated by HR through **RIT-102 Employee Starter Form**.
- This form will have the information of new employee and the access he or she required.
- In case of any movement from one campaign to another or from one department to other HR will inform us, so the access will be modified accordingly.
- HR will share the list of existing employees department wise with IT on quarterly basis which can be match up with the list of user account on the AD server and email server.
- In case of any discrepancy a security incident will raise to Information security manager.
- If any employee resigns, HR will proactively intimate IT by initiating separation notification and **RIT-101 Employee Transfer/Leaver Form** so his/her access rights will be revoked.
- Due to unique customer requirements, in case of employee resignation/transfer for business unit **Sybrid TS** business managers will share **RIT-204 TS Employee Leaver Transfer** form for separation process.

4.7.5. Anti-Malicious

4.7.5.1. Anti-Virus Setup

- Centralized Antivirus Server is deployed in our network to secure information facility from malicious viruses and Trojans.
- There is a client / server based solution so clients are not directly received their updates from internet and only internal server is responsible to receive all updates from Internet.
- Server is directly connected with the internet and downloads all necessary updates regularly.
- All Client PC's are fully scanned on weekly basis.

- Network sharing is also limited through antivirus server to ensure clean network.
- USB Mass storage Access is restricted with the help of Centralized Antivirus.

4.7.6. Drive Encryption

All laptops that carries company confidential information will have their drives Encrypted by using any Encryption scheme algorithm based software / Technique to maximize the security of data if incase of theft of employee's laptop.

4.7.6.1. Encryption Activity

- Using 3rd party Software or Microsoft windows features, System Support Engineer ensures the full drive encryption before handing over the laptop to the employee.
- System Support Engineers will make sure that all mobile devices storage media are encrypted with defined mechanism at the time of initial/re-configuration of device prior to handing it over to users.
- All encryption keys will be saved in a file and it will be placed at a centralized location accessible to all IT Team members.

4.7.6.2. Decryption Activity

- System Support Engineer must make sure the drive Decryption before performing OS Reinstallation, Drive Formatting & Drive Partitioning on employee's laptop to ensure data integrity & unwanted data loss.

4.7.7. Secure Communication and Infrastructure

There will be always secure communication channel would be provided if in case Sybrid needs to communicate with remote site or server that contains confidential data including EPHI.

4.7.7.1. Secure Infrastructure / LAN

All the internal servers and client machines would be at the back of a firewall that will ensure and maximize the protection and guard against the brute force attacks and vulnerabilities.

4.7.7.2. Secure Communication with Remote Sites & Customer Network

All the communication with remote Sites and customer network will be carried out with any of below mentioned two methods:

- Secure Site to Site IPsec VPN.
- Point to Point L3 MPLS connectivity.

4.7.8. Patch & Technical Vulnerability Management

Patch & Technical Vulnerability Management for all the Microsoft Operating Systems (Client/Server) shall be conducted by a centralized patch management system of Microsoft System Center Configuration Manager/ WSUS.

Only selected and important updates related to windows OS and software (Office, SharePoint etc.) are being reviewed and pushed by IT department and all systems are updated via windows automatic update.

If there is vulnerability identified/observed but there is no suitable countermeasure. In this situation, the Sybrid IT team should refer to forums and concerns subject matter experts depending on criticality of risks associated to such vulnerability and suggest appropriate corrective actions as suggested by such forums or subject matter experts and practice across the industry.

4.7.9. Resource Usage Logs

4.7.9.1. Internet Usage Log

Internet usage log will be maintained on Internet security Server and reviewed monthly by System Administrator using proxy server’s reports.

4.7.9.2. Access Control Log (like invalid login attempts on logon)

Access Control Logs will be monitored through system audit and policies by System Administrator by using server AD audit software.

4.7.9.3. Administrator Logs review

Manager IT/ AM IT shall review the logs of administrator privileged IDs on the following devices.

- Active Directory Servers by using AD audit software
- FTP/ File Servers by using AD audit software
- VoIP Servers by Linux default feature
- Application Servers by using AD audit software

4.8. Capacity Management

The use of resources should be monitored, tuned, and projections made for the future capacity requirements to ensure the required system performance.

4.8.1. Component Capacity Management

Alerts are configured on individual servers and a threshold is defined for hard drive, CPU and Memory utilization when the utilization exceeds the threshold it generates alert in event logs.

- System Engineer is responsible to perform regular maintenance activity to identify bottle necks and other issues.
- Utilization of resources is monitored on regular basis in maintenance activity such

as hard drive, CPU and Memory utilization.

- Event logs are also regularly monitored in maintenance and logged in maintenance reports.
- Any issues will be escalated to Manager/AM IT for further actions.

4.8.2. Service Capacity Management

Service Capacity management will be regular practice and IT will update the stake holders quarterly for Telephony, Internet, Email and other services through Service Capacity Report.

- IT will review the services according to the service capacity report on quarterly basis
- IT Manager will share the Service capacity report with all the stake holders.
- Stake holders will provide the approval on action items
- IT will proceed on action items and shared the updated service capacity report

4.8.3. Business Capacity Management

Business capacity management service capacity report will be shared with the BD Team and BD will share the new business forecast analysis so IT can ensure that future business requirements are translated into quantifiable IT services.

- IT will share the service capacity report with BD Team on quarterly or requirement basis.
- BD Team will share the new business forecast analysis on quarterly basis
- IT will share the action items according to the forecast analysis.
- Stake holders will provide the approval on action items
- IT will proceed on action items and shared the updated service capacity report.

4.9. Project Management

All the Projects of Sybrid IT can be distinguished in the following categories and any kind of change will be tackled through Change Management Process:

- Commercial Projects
- Commercial Expansion
- Internal Infrastructure

4.9.1. Commercial Projects

- Business Development Team provides complete Customer requirement to Sybrid IT Team ref: **RIT-210 Customer Requirement Form**.
- After receiving of **RIT-210 Customer Requirement Form**, Sybrid IT Team will design to complete infrastructure plan for the project as mentioned in **RIT-210 Customer Requirement Form** according to Customer needs.
- Any costing, pricing and solution must be reviewed by Sybrid IT Head.
- Sybrid IT will finalize action Plan to meet all the business requirements as per **RIT-227**

IT Project Action Plan.

- Manager/AM IT will ensure that all the requirements specified in **RIT-210 Customer Requirement Form** must be aligned with the **RIT-227 IT Project Action Plan** and will responsible for Project Delivery.

4.9.2. Commercial Expansion

- Business Unit Team provides complete Customer requirement with expected timelines to Sybrid IT Helpdesk System ref: **RIT-210 Customer Requirement Form**.
- After receiving of **RIT-210 Customer Requirement Form**, Sybrid IT Team will design to complete infrastructure plan for the project as mentioned in **RIT 210- Customer Requirement Form** according to Customer needs.
- Any costing, pricing and solution must be reviewed by **Sybrid IT Head**.
- Sybrid IT will finalize action Plan to meet all the business requirements as per **RIT-227 IT Project Action Plan**. This plan must be reviewed by Manager/AM I.T.
- Manager/AM IT will ensure that all the requirements specified in **RIT-210 Customer Requirement Form** must be aligned with the **RIT-227 IT Project Action Plan** and will responsible for Project Delivery.
- Manager/AM IT must ensure failback procedure in case of any disaster/failure that can occur after performing configuration.

4.9.3. Internal Infrastructure

- Any internal infrastructure upgrade, modification, enhancement or improvement must be presented by **RIT-228 IT Business case** to the Manager/AM I.T. by Sybrid IT Helpdesk System.
- Manager/AM I.T. will review it and approve/disapprove it considering its alignment with business, policies and procedures.
- Manager/AM IT will ensure that all the requirements specified in **RIT-228 IT Business Case** must be aligned with the **RIT-227 IT Project Action Plan** and will responsible for Project Delivery.
- Any costing, pricing and solution must be reviewed by Sybrid IT Head.
- Sybrid IT will finalize action Plan to meet all the business requirements as per **RIT-227 IT Project Action Plan**. This plan must be reviewed by Manager/AM I.T.
- Manager/AM IT must ensure that failback procedure in case of any disaster/failure that can occur after performing configuration.

4.9.4. System Acceptance before Deployment

- For Any project of any category appropriate system acceptance must be performed.
- Manager/AM IT will ensure that all the steps/actions are successfully taken according to the **RIT-227 IT Project Action Plan**
- According to the requirements contained in **RIT-210 Customer Requirement Form** Sybrid IT Team will provide the testing phase duration and after completion of the testing phase, Sybrid IT Team will share the testing results with Business Development team on **RIT-216 Testing Results**.
- After the successful testing, the project will be set in production to serve IT Services in LIVE environment.

4.10. IT Services Business Continuity & Disaster Recovery

- Sybrid IT Team must ensure onsite and offsite backups of all the information, Data and business critical services.
- A complete onsite & offsite backup plan for all the services, servers, information and data as per defined guidelines **GIT-203 Data Backup and Restoration Guideline** for Karachi and **GIT-303 Data Backup & Restore Guideline-ISB** for Islamabad**.**
- A comprehensive IT Disaster recovery plan is in place, which will be triggered in some certain scenario as defined in plan **Disaster Recovery Plan.**
- Systems Engineer/Administrator will test and ensure readiness of backups and DR services periodically as defined in **GIT-203 Data Backup and Restoration Guideline** for Karachi Infrastructure and **GIT-303 Data Backup and Restoration Guideline-ISB** for Islamabad Infrastructure.
- Systems Engineer/Administrator will ensure monitoring of defined onsite and offsite backups regularly and log their status in **RIT-218 Onsite Backup Log** and **RIT-219 Offsite backup log** as defined in **GIT-203 & GIT-303.**

5. Roles and Responsibilities:

Sr. No	Role	Responsibilities
1.	Manager I.T.	• Mentor/ Review/ approve/ architect design and enhancements in the Technology IT operation infrastructure and Services for entire business. • Being Lead of department for all regions will ensure all services uptime as per SLA.
2.	Assistant Manager I.T.	• Mentor/ Review/ approve/ architect design and enhancements in the Technology IT operation infrastructure and Services for particular site. • Being Lead for the region will ensure all services uptime as per SLA.
3.	Voice, Networks or Systems Administrator	• Maintain Voice, Systems & Network infrastructure / software troubleshooting inventory covering all the hardware resources. • Provide mentoring/ assistance to System/ System Support Engineer[s] in resolving problems. • Recommend & implement enhancements in the operational infrastructure after the design has been reviewed and approved by the Senior Technology Management Team. • Ensure all services uptime as per SLA.

4.	Voice, Networks or Systems Engineer	• To do operational level configuration, maintenance and monitoring on infrastructure network, servers and telephony systems as per the relevant task's SOP/ work plan/ Change request.
5.	Team Leads-Support	• Troubleshoot and resolve IT Operational support issues as per IT SOP which are escalated by System Support Engineers. • Ensure system support team is performing their day to day tasks, operations management, service desk management, change management and incident management as per IT SOP.
6.	System Support Engineer	• Troubleshoot and resolve IT operational support issues as per IT SOP. Ensure all queries on helpdesk and perform escalation according to their scope.

6. Associated Policies/Processes/Guidelines:

S. No.	Reference Number	Records Title
1	GIT-201	Infrastructure Configuration Management Guideline
2	GIT-202	Data Management Guideline
3	GIT-203	Data Backup and Restoration Guideline
4	GIT-204	Client End Configuration Guideline
5	GIT-301	Infrastructure Configuration Management Guideline-ISB
6	GIT-302	Data Management Guideline-ISB
7	GIT-303	Data Backup and Restoration Guideline-ISB
8	GIT-304	Client End Configuration Guideline-ISB

7. Associated Records:

Sr. #	Reference Number	Document Title
1	RIT-101	Employee Transfer/Leaver Form
2	RIT-102	Employee Starter Form
3	RIT-202	IT Requisition Form
4	RIT-203	Service Incident Report
5	RIT-204	Sybrid TS Employee Leaver/Transfer
6	RIT-205	Backup Inventory
7	RIT-209	IT Uptime Report

8	RIT-210	Customer Requirement Form
9	RIT-211	Maintenance Report
10	RIT-212	System Health Check Report
11	RIT-213	System Audit Report
12	RIT-214	Access Rights Form
13	RIT-215	Review Access Rights Form
14	RIT-216	Testing Results
15	RIT-217	Approved Software List
16	RIT-218	Onsite Backup Log
17	RIT-219	Offsite Backup Log
18	RIT-221	Daily UAN Audit Sheet
19	RIT-222	Daily Network Monitoring Sheet
20	RIT-223	Daily Server Monitoring Sheet
21	RIT-224	IT Resource Training Record
22	RIT-225	Daily IT Floor Checklist-Sybrid MD
23	RIT-226	Daily IT Floor Checklist-Sybrid CS
24	RIT-227	IT Project Action Plan
25	RIT-228	IT Business Case
26	RIT-229	Daily IT Floor Checklist-Sybrid TS
27	RIT-230	Privilege Access user List
28	RIT-231	Disposal List
29	RIT-232	Data Center Visitors Log Sheet
30	RAD-403	Stock issuance & purchase requisition
31	RISM - 913	Change Management Form