Office of the Principal Accountant General

Gujarat

MANUAL

OF

INFORMATION TECHNOLOGY MANAGEMENT GROUP (ITMG)

PREFACE

This manual has been prepared for internal use in the Office only. It embodies the procedure to be followed in the day to day functioning of the ITMG section. The instructions, procedures contained in this manual are supplementary to the instructions issued by the Comptroller and Auditor General of India from time to time.

The staff may take the advantage of the material in this manual to keep themselves acquainted with the rules and procedures.

Suggestions either in the nature of amendments to or rectification or omission, if any, should be brought to notice of the SAO, ITMG who would be responsible to ensure that this manual is kept up to date.

Ahmedabad

Date : _____

Principal Accountant General (E&RSA
Gujarat

CHAPTER - 1

INTRODUCTION

The Indian Audit and Accounts Department is headed by the Comptroller and Auditor General of India with Headquarters at New Delhi. The office of the Accountant General (Audit-I) came into existence with effect from 1st march, 1984 on restructuring of the erstwhile Audit Department. Consequent upon restructuring of the Audit offices in Gujarat in March 2012, the office has been named as Office of the Principal Accountant General (Economic & Revenue Sector Audit). The office of Principal Accountant General (E&RSA) is under the overall supervision and control of the Principal Accountant General.

Information Technology Management Group being a part of establishment comes under the direct charge of Senior Deputy Accountant General (Admn) / Deputy Accountant General (Admn). Senior Audit Officer (ITMG)/Audit Officer (ITMG) is designated as the branch officer of the ITMG section and Assistant Audit Officer ITMG is the section in-charge of the ITMG section.

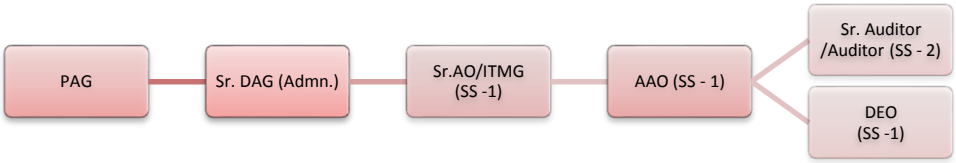

Fig1.1 Organizational Chart

1.1 The functions of ITMG are as follows:

1.1.1 IT Support Cell :

The ITMG section is entrusted to provide direct IT related assistance and support to different sections in the Office. IT support includes giving technical assistance for issues related to day to day operation of various IT equipments. All the IT related complaints are handled by the ITMG section. Further, various in house softwares are also developed based on the requirement of the users. Software related issues viz. installation of OS, Application software, third party software, etc. are also handled on a day to day basis.

1.1.2 Managing IT Resources (Hardware, Software and Network) :

All the purchases relating to IT Hardware viz. Computer, Laptops, Printers, Scanners Network Switches etc. including other consumables for use in the Office are done by ITMG Section. Various software viz. Operating System, Application software, etc. for use in the Office are also procured through ITMG Section. These purchases are done from the separate fund maintained under the head “Information Technology”. The maintenance, repair and

upkeep of these hardware and software on a regular basis is done through the ITMG section.

The inventory of all the Hardware and Software available in the Office is maintained in the Stock register in a prescribed format. This stock is maintained in the MS Access database containing the details about configuration, date of purchase, vendor, purchase price, section, etc. This information is also updated in the Online Inventory module on the C&AG website.

The networking viz. Local Area Network, Internet, etc. for the office use is maintained by the ITMG Section. Purchase and installation of various Network equipment viz. switches, Modems, Firewall, etc. including laying of cabling and setting up of Network points are done. Internet connection is obtained from Internet Service Provider and shared among the users in the office according to the Internet Policy. Regular maintenance and upkeep of the network equipment is also taken care of.

1.1.3 IT Security Policies :

Various IT Policies are implemented in the Office as per the instructions issued from Headquarters office from time to time. These policies include General IT Policy and specific IT Policies for Antivirus, Backup, Network, Email, Internet, etc. The framework of these IT Policies are derived from the IT Security Hand Book issued by Headquarters office.

1.1.4 Server Management :

Server is the critical component in the IT infrastructure. As servers needs to be run on 24 X 7 basis these are installed and maintained under the direct supervision of the ITMG Section. The server includes Data Server, Email Server, Internet Server, Application Server etc. Critical administrative functions including user management, antivirus management, rights management, security management are directly done with the help of an outsourced technician.

1.1.5 Development and Updation of Office Website:

The office website is hosted on the NIC domain (GOV.IN). It has been developed in house by the ITMG section in the ASP.NET platform. The VPN authentication and digital signature has been obtained in the name of the Sr. DAG (Admn.). The content of the website is regularly updated based on the changes recommended by Website committee and approved by the PAG. The corresponding Hindi portion of each webpage is also updated as recommended by the Hindi Website committee and approved by the PAG.

1.2 Return Submitted by the ITMG are as follows: -

Part: - I Daily

1	Attendance Register	Branch Officer

Part: - II Weekly Submission

1	Inward Register	Branch Officer
2	Calendar of Register	Sr.AO/AO

Part:-III Fortnight Submission

1	Outward registers	Branch Officer

Part: - IV Monthly Submission

1	Arrears Report	Q.A. Section
2	Closing of Attendance Register	Branch Officer
3	Monthly Performance	PAG
4	Calender of Return	Group Officer
5	Departmental Note Book	Group Officer
6	Back Up Register	PAG

Part: -V Quarterly Submission

1	AAOs/ SOs Note Book	B.O
2	Auditors Note Book	B.O.
3	IT Status Project -8	PAG
4	Calender of Returns	Q.A. Section
5	Physical Verification Of Articles	GOM
6	policy for domestically manufactured Electronic Products	Hqrs.
7	Director of Inspection	Q.A. Section

Part: - VI Half Yearly Submission

1	Utilisation of Assets of Hardware and Software.	CAG Office

Part: - VII Annual Submission

1	पर्श्नावाली सम्बंधित प्रफोर्मा	हिंदी अनुभाग
2	Physical Verification of IT Assets	PAG

CHAPTER - 2

IT SUPPORT CELL

The ITMG is entrusted with the responsibility of providing required IT Support to the different sections/wings on a day to day basis. The support includes hardware, software, networking, database, programmes, development, etc. The various support assistance provided is as follows:

2.1 Hardware Support:

- Attending the problems related to the non-functioning of the Computers, Laptops, Printers, Scanners, etc.
- Regular maintenance of various IT Equipments for smooth functioning of the same.
- Up gradation of the Hardware on need to know basis.
- Arranging for the repair of the various IT Equipment.
- Arranging for the refilling and purchase of consumable parts for printer on day to day basis.

2.2 Software Support:

- Arranging for installation of various Application software viz. MS Office, Printer software, Scanner software and other third party software.
- Attending to problems viz. reinstallation, formatting, repairing etc. pertaining to the Operating system.
- Attending to the problems related to technical usage of various software viz. MS Word, MS Access, MS Excel, etc.
- Managing users for DAK management system, including creation, deletion, Updation of users.

2.3 Networking Support:

- Providing networking to computers, Laptops, printers, etc. on need to know basis.
- Attending to the problems relating to non-functioning of the Local Area Network. (LAN)
- Attending to the problems relating to Internet, GSWAN, etc.
- Providing Wi-Fi to the various officers on need basis.
- Managing users for LAN access, including creation, deletion and updation of the users.
- Managing rights management for the access of various resources on the Network.
- Managing rights management in the firewall for the access to the Internet on need to know basis.

- Managing user for Round cube (Intranet Email).

2.4 **In-house Programme support:**

ITMG section is also involved in the development of in-house software for various users/sections for day to day activities. These softwares include IR Main, Pay Bill Software, GPF Package, Contingency Bill Package, etc. These programmes have been developed in MS Access. The regular updation, development, maintenance of these programmes are managed by the ITMG section.

2.5 **Other Support:**

2.5.1 **Storage Services*:*** ITMG section provides storage drive (S: Drive) to all wings/sections of the office. Each section has been provided separate folder on the server for storing and retrieving the data pertaining to that section/wing. Each section/wing has been provided with separate authentication for officers and staff for accessing the server. Hence, the data is accessed by authorised users only.

2.5.2 **Internet Services:** ITMG section provides the internet connection to all wings/sections in the office. For this purpose, multiple internet connection (Broadband connection) has been acquired from BSNL and is shared using the Firewall (Cyberoam). The internet connection is shared based on a need to know basis. Various firewall rules have been framed (as approved by Principal Accountant General) for the different level of users so that unauthorised and misuse of the internet can be prevented.

2.5.3 ITMG section provides necessary support to the field staff in solving various issues relating to Laptops, software, virus etc.

2.5.4 In-house training is also imparted by the ITMG section which includes Basic IT knowledge as well as advanced courses in MS Access, MS Excel, MS Word, etc.

2.5.5 Regular Backup of the server data is taken on daily basis to another local computer. Further, as per IT policy the Full backup of the server data is stored Bi-monthly in DVD/External Hard drive and stored in a remote location under the safe custody of Office of the AG (G&SSA) Rajkot.

CHAPTER - 3

MANAGING IT RESOURCES (HARDWARE, SOFTWARE & NETWORKING)

All IT Hardware, Software and Networking resources pertaining to the office are managed by ITMG section. Hardware includes Computers, Laptops, Scanners, Printers, Projectors, etc. Software includes various System software, Application software, Third party software, etc. Network includes the LAN containing Network switches, Modems, Firewall, Cabling, etc.

Managing IT Hardware includes procurement of new IT Hardware, Inventory Management and periodic Maintenance & Repairs.

3.1 Procurement of IT Hardware and Software

All the purchases relating to IT Hardware viz. Computer, Laptops, Printers, Scanners, Network Switches, etc. including other consumables for use in Office are done in ITMG Section. Softwares viz. Operating System, Application software, etc. for use in the office is also procured through ITMG Section. These purchases are done from a separate fund maintained under the head "Information Technology".

3.1.1 Every year at the starting of the financial year, the requirement for various IT Hardware and Software including networking is called for from various sections/wings and is compiled and approved by the Principal Accountant General for sending to Headquarters office. These requirements are prepared taking into consideration the requirement for the whole year so as to avoid piece meal requirement being sent to Headquarters office. These requirements are compiled in the prescribed format Annexure – A to D as prescribed by Headquarters office. These requirement includes funds for purchase of new IT Equipment & software, AMC, consumables, etc. The requirement of funds must be accompanied by the position of the hardware infrastructure and software available in the Office, which should be in unison with the data entered in the Online Inventory Module maintained online with the CAG office. Further, a certificate by Sr.DAG/DAG (ITMG) should also be attached stating that the IT Assets in the office confirms with the Online Inventory Module.

Based on the requirement sent to Headquarters office (Principal Director/IS), the funds are released by the BRS wing in CAG office after administrative approval from PD/IS.

Items available under DGS&D rate contract are procured from the authorised vendors under the prescribed terms and conditions mentioned in the DGS&D rate contract. In no case the items should be purchased below the configuration mentioned by the Hqrs. Office.

In case of any Rate Contract being entered with the CAG office for supply of any item, the purchase order for such items can be placed

directly with the authorised vendor on the prescribed format attached to the Rate Contract.

3.1.2 All other purchases are done as per provisions of GFR 2005 chapter on Procurement especially (Rules 149to 154). Important extracts of some of the Rules from GFR are as below:

a) **Rule 149. Purchase of goods by obtaining bids:** Except in cases covered under **Rule 145, 146 and 147(1),**

Ministries or Departments shall procure goods under the powers referred to in **Rule 140** by following the standard method of obtaining bids in:

(i) Advertised Tender Enquiry;

(ii) Limited Tender Enquiry;

(iii) Single Tender Enquiry.

b) Rule 150. Advertised Tender Enquiry.

(i) Subject to exceptions incorporated under **Rules 151 and 154**, invitation to tenders by advertisement should be used for procurement of goods of estimated value Rs. 25 lakh (Rupees Twenty Five Lakh) and above.

Advertisement in such case should be given in the Indian Trade Journal (ITJ), published by the Director General of Commercial Intelligence and Statistics, Kolkata and at least in one national daily having wide circulation.

(ii) An organisation having its own web site should also publish all its advertised tender enquiries on the website and provide a link with NIC web site. It should also give its web site address in the advertisements in ITJ and newspapers.

(iii) The organisation should also post the complete bidding document in its web site and permit prospective bidders to make use of the document downloaded from the web site. If such a downloaded bidding document is priced, there should be clear instructions for the bidder to pay the amount by demand draft etc. along with the bid.

(iv) Where the Ministry or Department feels that the goods of the required quality, specifications etc., may not be available in the country and it is necessary to also look for suitable competitive offers from abroad, the Ministry or Department may send copies of the tender notice to the Indian embassies abroad as well as to the foreign embassies in India. The selection of the embassies will depend on the possibility of availability of the required goods in such countries.

(v) Ordinarily, the minimum time to be allowed for submission of bids should be three weeks from the date of publication of the tender notice or availability of the

bidding document for sale, whichever is later. Where the department also contemplates obtaining bids from abroad, the minimum period should be kept as four weeks for both domestic and foreign bidders.

c) Rule 151. Limited Tender Enquiry

(i) This method may be adopted when estimated value of the goods to be procured is up to Rupees twenty five Lakhs. Copies of the bidding document should be sent directly by speed post/registered post/courier/e-mail to firms which are borne on the list of registered suppliers for the goods in question as referred under **Rule 142**. The number of supplier firms in Limited Tender Enquiry should be more than three. Further, web based publicity should be given for limited tenders. Efforts should be made to identify a higher number of approved suppliers to obtain more responsive bids on competitive basis.

(ii) Purchase through Limited Tender Enquiry may be adopted even where the estimated value of the procurement is more than Rupees twenty-five Lakhs, in the following circumstances.

- The competent authority in the Ministry or Department certifies that the demand is urgent and any additional expenditure involved by not procuring through advertised tender enquiry is justified in view of urgency. The Ministry or Department should also put on record the nature of the urgency and reasons why the procurement could not be anticipated.
- There are sufficient reasons, to be recorded in writing by the competent authority, indicating that it will not be in public interest to procure the goods through advertised tender enquiry.
- The sources of supply are definitely known and possibility of fresh source(s) beyond those being tapped, is remote.

(iii) Sufficient time should be allowed for submission of bids in Limited Tender Enquiry cases.

d) Rule 153. Late Bids:

In the case of advertised tender enquiry or limited tender enquiry, late bids (i.e. bids received after the specified date and time for receipt of bids) should not be considered.

e) Rule 154. Single Tender Enquiry

Procurement from a single source may be resorted to in the following circumstances:

(i) It is in the knowledge of the user department that only a particular firm is the manufacturer of the required goods.

(ii) In a case of emergency, the required goods are necessarily to be purchased from a particular source and the reason for such decision is to be recorded and approval of competent authority obtained.

(iii) For standardisation of machinery or spare parts to be compatible to the existing sets of equipment (on the advice of a competent technical expert and approved by the competent authority), the required item is to be purchased only from a selected firm.

Note: *Proprietary Article Certificate in the following form is to be provided by the Ministry/Department before procuring the goods from a single source under the provision of sub* ***Rule 154 (i) and 154 (iii)*** *as applicable.*

(i) The indented goods are manufactured by M/s……..……..

(ii) No other make or model is acceptable for the following reasons:

……
……
……
……

(iii) Concurrence of finance wing to the proposal vide : ……..

(iv) Approval of the competent authority vide : .. …….……

_____

(Signature with date and designation of the procuring officer)'

3.2 The purchases are also governed by the GOI Ministry of Communications and Information Technology OM No.33(3)/2013-IPHW circulated by CAG Hqrs Circular Letter No.1258/ISW/154/2015 dated 9-7-2015 regarding "Policy to provide preference to domestic manufacturers – Sole selling agents/authorized distributors/ authorized dealers/authorized supply houses of domestic manufacturers".

3.3 Inventory of Hardware and Software

For effective management of the IT resources, details of all the IT hardware and software available in the office is maintained in the Stock Register in a prescribed format. The stock register is maintained in the MS Access database separately for Computer, Laptop, Printer, Scanner, Projector, Switches, etc. It contains the details about configuration, date of purchase, vendor, purchase price, section to which alloted, etc. The software register is also maintained containing the list of all the available software with the office and details of the licence, date of procurement, price, etc. The Inventory details are also maintained in the Online Inventory module on the CAG website.

The following entries are entered/updated on the Inventory on regular basis:

- New procurement of the IT Hardware and software.

- Disposal of old IT Hardware not in use.
- Allocation/Reallocation of the IT Hardware within the sections/wings
- Any changes in the Hardware configuration, network, software due to upgradation.

3.4 Maintenance and Repairs

For the upkeep of all IT Hardware and Software regular maintenance, repairs and up gradation is done by the ITMG Section. The following activities are initiated in this regard.

- Preventive maintenance of all the IT Hardware is done on a regular basis (Annual contract) through outsourced vendors.
- Repairing is done on a day to day basis based on complaints received from the users.
- Replacement of defective parts.
- Refilling and parts replacement of Printers.
- Formatting and reinstallation of Operating System.
- Reinstallation of the Application programmes.
- Conducting system scan, network scan, etc for detecting the various issues in the Computer.
- Up gradation of the RAM, Network card, Processor and Mother Board of the Computers.
- AMC contract on annual basis and their engineers work on call basis.

3.5 Managing Network resources

The networking viz. Local Area Network, Internet, etc. for the office use is maintained by ITMG Section. Purchase and installation of various Network equipments viz. switches, Modems, Firewall, etc. including laying of cabling and setting up of Network points are done. Internet connection is obtained from Internet Service Provider and shared among the users in the office according to the Internet Policy. Regular maintenance and upkeep of the network equipments is also taken care of.

3.6 Physical Verification of IT Hardware & Software.

As per Rule 192 of GFR 2005, annual verification of the assets needs to be carried out annually. Physical verification is carried out by ITMG every year in the month of April/May by Group Officer of any other Office, nominated by PAG.

CHAPTER - 4

IT POLICIES

4.1 Preamble

ITMG section has an obligation to ensure appropriate security for all Information Technology data, equipment, and processes under its control.

4.1.1 The purpose of the IT Policies mentioned hereunder is to create an environment that ensures security of various IT equipments, maintain system security and availability, data integrity, and individual privacy by preventing unauthorized access to information and information systems and by preventing misuse of, damage to, or loss of data.

4.1.2 The Information Systems Security Handbook published by CAG of India in December 2003 lays down the basic requirements of IT security and various policies to be adopted in IAAD. It explains various concepts, policies and compliance mechanism for securing information resources. It also lays down threshold requirements based on International standards and ISO 17799.

4.1.3 All the IT policies e.g. Password policy, Anti-virus policy including domain Specific Security instructions, Subsidiary Security Policies, etc. as specified in this hand book apply to all the offices of IAAD across the country. The ITMG section implements these policies in this office after necessary approval from the Competent Authority. Sr. Dy. Accountant General (Admn) in charge of the ITMG section has been nominated as the IT Security Officer in this office.

4.1.4 The above mentioned IT Policies are meant to:

- Enumerate the elements that constitute IT security.
- Explain the need for IT security.
- Specify the various categories of IT data, equipment, and processes subject to this policy.
- Indicate, in broad terms, the IT security responsibilities of the various roles in which each member of the Department may function.
- Indicate appropriate levels of security through instructions in the form of policies and guidelines.

The Information System Security Handbook for IA&AD is available at the following web link:

http://www.saiindia.gov.in/english/home/Public_Folder/Manuals/ISW/IT_S/IT_S.html

4.2 Password policy:

4.2.1 In compliance of the instructions mentioned in the Hand book, in order to establish a standard for creation of passwords, the protection of the passwords and to prescribe the frequency of change of passwords, a

Password policy has been implemented in this office. The same prescribes that:

- Strong passwords containing both upper and lower case characters and digits and punctuation characters are to be chosen for systems and emails etc and the passwords less than eight characters, common usage words and dictionary words, names of family, friends, pets, birthdays are to be avoided.
- Passwords are to be never written down or stored on line.
- All system-level passwords must be changed at least on quarterly basis. All user-level passwords must be changed at least every six months. The recommended change interval is four months.
- Passwords are not being shared with others
- Separate passwords are to be used for IAAD and non IAAD access.
- Remember password feature of applications should not be used.

4.3 Antivirus policy

In order to maintain data integrity and to establish security requirements which need to be met by all stand-alone computers and computers connected to Network and to ensure virus detection and prevention, an Anti-virus policy has been implemented in this office by ITMG section. The said policy is applicable to Desktop computers, laptops file, ftp, proxy servers etc.

As per Antivirus policy all IAAD PC based computers must have IAAD's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the Antivirus software and the virus pattern files must be kept up to date.

It is the responsibility of the primary user of the PC to ensure that anti-virus software is updated regularly. Virus infected computers must be removed from the network until they are verified as virus free. Any activities with the intention to create and/or distribute malicious programmes into IAAD's networks are prohibited.

(Circular No. ITMG/05/2012-13 dated 24.12.2012)

4.4 Policy on use of IT Resources

The policy on use of IT Resources of Government of India, issued by Ministry of Communication and Information Technology (Department of Electronics and Information Technology), New Delhi and circulated by CAG's Office on 16th March 2015, governs the usage of IT resources from an end user's perspective.

The objective of this policy is to ensure proper access to and usage of Government's IT resources and prevent their misuse by the users. Use of resources provided by Government of India implies the user's agreement to be governed by this policy.

The following domains are covered under this policy:

- Access to Internet and Intranet

- Access to Government Wireless Networks
- Filtering and block of sites
- Monitoring and Privacy
- Email access from Government Network
- Access to Social Media sites from Government Network
- Use of IT Devices issued by Government of India

The said policy of Government of India is available at the web link http://deity.gov.in/sites/upload_files/dit/files/Policy%20on%20use%20of%20IT%20resources%20of%20Government%20of%20India.pdf

In order to outline the acceptable use of computer equipments and to protect employees and the Department from illegal or damaging actions by individuals, either knowingly or unknowingly, the Information Technology Acceptable Use Policy has been implemented in this office.

4.5 As envisaged by Headquarters office, in order to outline acceptable use of computer equipments at IAAD, these rules have been enacted to protect the employees and the department from inappropriate use and avoid risks such as virus attacked, compromise of network systems and services and other legal issues. As per policy for acceptable use of IT resources, inter-alia it has been prescribed that:

- Employees are responsible to exercise good judgment regarding reasonableness of personal use. The criteria for misuse of Government resources should govern the action of the employee.
- Any information that users consider the sensitive or vulnerable be encrypted.
- Internet resources should be properly used and violation of any law should be avoided.
- The unacceptable uses of IT resources include the following activities:
- Violation of rights or a person or company trade secret etc
- Unauthorized copying of copyrighted material
- Installing of freeware/shareware on IAAD computer resources without permission
- Using IAAD computing assets to engage in transmitting material that may be construed as sexual harassment or creating hostile environment
- Effecting security breaches or disruptions of network communication
- Circumventing user authentication or security
- In order to implement the policies related to Internet and use of IT resources, the Cyberoam security system is used by the ITMG section to regulate the user access to internet resources.

4.6 Email Policy

In order to ensure secure access and usage of Government of India e-mail services by its users, the Email policy was issued by Ministry of Communication and Information Technology (Department of Electronics and Information Technology), New Delhi. The same was circulated by CAG's Office on 16th March 2015 with instructions to comply the same.

As per abovementioned email policy, only the e-mail services provided by NIC, the Implementing Agency of the Government of India shall be used for official communications by all organizations except those exempted under clause no 14 of this policy. The e-mail services provided by other service providers shall not be used for any official communication.

The email policy of the Government of India is available at the web link: http://www.deity.gov.in/sites/upload_files/dit/files/Gazette_notification_of%20E-mail_Policy_of_Government_of_India.pdf

In pursuance of Headquarters office instructions this office has implemented the email policy which inter-alia lays down on the following major points:

4.7 Responsibilities of Users:

a. The User is responsible for any data/e-mail that is transmitted using the GoI e-mail system. All e-mails/data sent through the mail server are the sole responsibility of the user owning the account.

b. Sharing of Email passwords is prohibited.

c. Users shall be responsible for the activities carried out on their client systems, using the accounts assigned to them.

d. The 'reply all' and the use of 'distribution lists' should be used with caution to reduce the risk of sending e-mails to wrong people.

e. Back up of important files shall be taken by the user at regular intervals.

4.8 The inappropriate Uses of E-mail Service include:

a. Creation and exchange of e-mails that could be categorized as harassing, obscene or threatening.

b. Unauthorized exchange of proprietary information or any other privileged, confidential or sensitive information.

c. Unauthorized access of the services. This includes the distribution of e-mails anonymously, use of other officers' user ids or using a false identity.

d. Creation and exchange of advertisements, solicitations, chain letters and other unofficial, unsolicited e-mail.

e. Creation and exchange of information in violation of any laws, including copyright laws.

f. Wilful transmission of an e-mail containing a computer virus.

g. Misrepresentation of the identity of the sender of an e-mail.

h. Use or attempt to use the accounts of others without their permission.

i. Transmission of e-mails involving language derogatory to religion, caste, ethnicity, sending personal e-mails to a broadcast list, exchange of e-mails containing antinational messages, sending e-mails with obscene material, etc.

4.9 Restriction on transmission of official and unauthorised information over social networking websites

The usage of social networking websites like "Facebook", "Twitter" etc. has been totally prohibited in the office and the officials have been instructed not to put forth office matters in public domain. Any violation of these instructions is to be viewed seriously and the accordingly appropriate action will be taken.

(Authority: Hqrs. office Letter No. 169/3-PPG/2011 dated 22.05.2012)

4.10 The said instructions of Headquarters office regarding transmission of official and unauthorised information over social networking websites have been circulated and the implementation of the same is watched by the ITMG section.

- In addition to the above, the following activities are being carried out by the ITMG section in respect of IT policies:
- Circulating the policy details to all the IT users for awareness on regular basis.
- Implementation of various rules for the internet access in the firewall.
- Implementation of usage of strong and complex passwords on the computer systems installed in the office.
- Regular review of the logs generated by the Firewall and servers for checking the compliance of the policy.
- Ensure proper identification and security aspects of various IT Equipments installed in the office.

CHAPTER - 5

SERVER MANAGEMENT

The different server in the office are installed and maintained under the direct supervision of the ITMG Section. The server includes Data Server, Email Server, Internet Server, Application Server etc. Critical administrative functions including user management, antivirus management, rights management, security management are directly done with the help of outsourced technician.

The following servers are managed by ITMG:

Data Server – Windows Domain Name System, Data Storage, Windows User management and Rights Management, etc.

Internet Server – Internet sharing, Firewall, Internet User management and Rights management.

Antivirus Server – Antivirus to client machines

Dak Server - Dak Management SQL services including storing, retrieving and processing for DAK application.

Email Server - Intranet Email Communication

5.1 Data Server

The data server has been configured on the Windows server 2012 platform. It performs the following functions and provides the following services:

- It acts as the Domain Name System in the Local Area Network. It contains the entry of all the local client machines with the network name and helps in identifying the computers on the network.
- It helps in user management. All the client user account available on the network are managed in this server. It facilitates creation and deletion of the user account. Group users are also created for group management.
- It facilitates management of user rights. Different users are given permissions based on the policy of the department.
- It facilitates the storing, retrieving and processing of data on the centralised data storage s: drive. The biggest advantage of the Centralised data storage is that any user can log in to any of the computer on the network and access their data.

5.2 Internet Server

The internet server is hardware (Firewall). The internet server acts as the gateway for accessing the internet on the network. All the users on the

network get access to the internet based on their requirement and policy implemented.

The following are the basic functions/facilities provided by the Internet Server.

- It facilitates the internet user management. Different internet users can created and deleted based on the requirement. These users can login to the firewall using the client software and get the access to the internet.
- It facilitates sharing of multiple internet connections. Presently two broadband connections have been configured for use in the office.
- It facilitates user's rights management. Depending on the policy different internet users can be provided different access rights based on the time, data size, speed, etc. Presently, four level of users has been created viz. clientless users for Group A officers, Super end users for Sr. AO/AO, High end users for AAO and normal users for sections.
- It facilitates as gateway for any connection to the Local Area Network. It is the single point of entry in the Local Area Network.
- It facilitates as firewall. The firewall acts as a wall between the outside and inside network. Hence, it protects from the outside attack from intruders. The internal configuration of the network is kept unknown to the outside network, preventing it from hacking of the computers on the LAN.

5.3 Antivirus Server

The Antivirus server is the server which facilitates the installation and setting up of the antivirus on the different client computers on the network. The antivirus server acts as the single point of access for the effective and efficiently management of the antivirus need in the department. Presently, we have installed the Kaspersky Antivirus Protection for the purpose.

The main functions/facilities provided by the Antivirus server are:

- It facilitates easy setting up of the antivirus software on client computers which are connected to the LAN. The antivirus is installed on the client computer using the admin console tool on the Antivirus server.
- It facilitates license management for the antivirus. The license is scalable i.e. it can be increased based on the requirement in future.
- It facilitates easy updation of antivirus database. Only the antivirus server needs to be updated online. All the updates installed on the antivirus server get automatically updated on the client machines.
- It facilitates easy maintenance of the antivirus software. All infected computers can be scanned centrally through admin console on the antivirus server.

5.4 DAK Server

The Dak server has been installed for the working of DAK Management System provided by the CAG office for the use in the Office. This system

helps in the effective management of the DAK received in the office. The server runs on SQL Server database with VB DOT NET on the front end. The users can access this programme on Internet Explorer 10 or above version.

The following are the key functions provided by the DAK Server:

- Facilitates the indexing of the letters received in various wings/sections.
- Facilitates effective management of the Inward Register.
- Facilitates the searching of letter based on subject, date, from, etc.
- Facilitates the generation of arrear report.
- Facilitates the generation of various reports for the use in sections.
- Facilitates the proper maintaining of the Inward register through printouts from the software.

5.5 Email Server

The Email server has been hosted in house in the UNIX platform. The server is managed by ITMG section though outsourcing. The Email server runs on 24 X 7 basis except under preventive maintenance. The server has been configured on Core i3 processor with 4 GB RAM. There is no limitation of the number of users on the Email Server. Presently, the Email server is common between the PAG (E&RSA) office and PDA office, hence enabling for easy intranet email among the users of both the offices. Due to limitation of the space, the users has been given a limit of 300 MB of storage on the Email Server. The storage is 500 MB for Group A Officers.

The following are the functions of the Email server:

- Facilitates the internal correspondence through Email within the Office.
- Facilitates secured email as it is available only on LAN.
- Facilitates the creation/deletion of the users on need to know basis as it is hosted in house.
- Facilitates Email management through Outlook.

CHAPTER 6

WEBSITE MANAGEMENT

The office website is hosted on the NIC domain (GOV.IN). It has been developed in house by ITMG section in the ASP.NET platform. The VPN authentication and digital signature has been obtained in the name of the Sr. DAG (Admn.). The content of the website is regularly updated based on the changes recommended by Website committee and approved by PAG. The corresponding Hindi portion of the each webpage is also updated as recommended by the Hindi Website committee and approved by PAG. The website committee (English & Hindi) is nominated by PAG, which consists of three Sr. AO/AO at members.

The following are the requirements/guidelines/policy to be followed for the Computer identified for the Website update.

6.1 Software

Operating system not below Windows 8 is recommended. The Visual Studio, Dot Net Version 10 and above is recommended. The source code is accessible in Visual Studio version 10 and above.

6.2 Hardware

Any computer above CORE i3 processor with more than 2 GB RAM is recommended for the purpose of using the Visual Studio, Net programme.

6.3 Security

This computer is required to be protected by a strong password and should be physically out of reach of the normal users. Only ITMG officials should have the access to this computer.

6.4 Domain Registrar

The office website has been hosted on the NIC server on domain GOV.IN. The NIC is the domain registrar for the GOV sites. In this regard, the registration has been obtained from the NIC by this office which is required to be renewed every two years. The renewal request is required to be processed thru Sr. Technical Director/NIC at Gandhinagar well in advance i.e. at least 2 months before expiry so that it is ensured that the same domain name is not issued to some other organisation.

6.5 Digital Signature & VPN Connection

Any changes in the material of website is done by the ITMG section and uploaded on the NIC server. For accessing the NIC server, this office has been provided the Digital Signature in the name of the Sr.DAG/Admn for identification of the user. The connection to the NIC server is established by a secured connection through VPN connectivity. This office has been provided the VPN authentication for

this purpose. The Digital signature is required to be renewed every 3 years from the NIC. The renewal form for the same is required to be processed thru Sr. Technical Director/NIC at Gandhinagar well in advance before the expiry of the Digital Signature.

6.6 FTP file transfer

The webpages are uploaded on to the NIC server thru FTP programme. For this any available FTP software can be used after establishing secured connection through VPN. This office uses file Zilla software for the FTP. The NIC has provided a separate authentication for the accessing the NIC FTP server to this office.

6.7 Procedure for Updation

The following procedure is followed for the regular updation of the website:

(i) The material for the updation of the website if any is compiled by the ITMG Section based on the changes being noticed from time to time.

(ii) The same is then submitted to the Website Committee on a regular basis (bi-monthly). The Website committee goes through the required changes and also suggest additional changes if any.

(iii) The changes recommended by the Website committee are then submitted to Sr.DAG/ITMG for approval, which is then submitted to Pr.A.G. for approval.

(iv) After the approval of the Pr.A.G., the corrections/updation is carried out by ITMG section.

(v) After correction/updation in the material, the website is published on to the NIC server.

(vi) After approval of the English material of the website, the corresponding Hindi material is sent to Hindi Section for translation and typing.

(vii) On arrival of material from Hindi Section, the same is then uploaded on the website by ITMG section.

6.7.1 Important Checks

The following checks should be exercised during updation of the website:

- ✓ Ensure that a separate folder is created for source in every instance of change.
- ✓ Ensure that the source and published/complied WebPages of that source is stored on the same folder.
- ✓ Ensure that the VPN authentication, Digital Certificate, FTP authentication details are not shared with anybody outside and remains within the ITMG officials.
- ✓ Ensure that the backup of the source as well as published/compiled web pages are taken before updation on the live server on NIC.