NATIONAL TELECOMMUNICATION AND INFORMATION SECURITY BOARD

POLICY FOR INTERNET, INTRANET, WEB-SITES AND E-MAIL IN FEDERAL GOVERNMENT ORGANIZATIONS

CABINET DIVISION

<u>General</u>

1.   The Government of Pakistan encourages the Government organizations and their employees to use e-mail, Internet, organizational websites and other means of electronic media to conduct the business of Government, to communicate with other officers within Government and with the general public, to gather information relevant to their duties, and to develop expertise in using such tools and services. The continued effort of the relevant departments is gradually shifting the functioning of the government offices to paperless environment. A number of steps have been taken while others are in progress to provide necessary hardware and software to equip all offices of the Federal Government to use these modern tools to enhance their proficiency and improve the responses to public demands.

2.   While the modern tools and services have enormous facilitation, they pose great vulnerabilities to the systems through inadvertent or deliberate actions by organizations or individuals in disclosing classified information in an unauthorized manner or for unlawful activities.   There is thus a need to lay down policy framework for the government organizations to use these tools and services in an organized manner to ensure security of information and network. Cabinet Division in consultation with various stake holders, and with the assistance of technical and security related organizations is instituting this policy to help Government organizations/individuals to get benefit from use of E-mail, Internet and organizational Websites, in a manner that it does not compromise national security.

3.   The intention of this policy is to establish a culture of openness, trust, integrity and not to impose unnecessary restrictions. The systems covered in the policy are to be used for official business in serving the interest of Federal Government and its operations. Effective security is a team effort involving the participation and support of every employee and affiliate who deals with the information and/or information systems. It is the responsibilities of every computer user to follow these guidelines, in letter and spirit to ensure optimum efficiency without compromising security of official information.

<u>Policy Objectives</u>

4.   The policy aims at meeting following objectives:

     a   To provide guidelines to government organizations on use of electronic ways of communications (E-mail, file servers, web sites/portals) for exchange of unclassified official correspondence in a controlled and efficient manner.

     b   To illustrate essential hardware/software required to establish an E-mail exchange/ Internet infrastructure.

     c   To lay down security parameters for use of Internet/E-mail.

d	To institute a system of periodic technical audit to assist government organizations, establish and maintain secure and reliable data network environment.
e	To provide broad guidelines on creating departmental security standards to ensure network/system (software/hardware) security.

Applicability

5.   The policy essentially applies to the following:

a	All Government Organizations under the Federal government, which will be connected to the Federal Government Intranet.
b	Provincial Governments and other organizations may use this policy as a guideline to draw up respective policies.
c	For exchange of unclassified information only as defined in the documents on Handling of Classified Matters in the Government Departments.
d	In the event of a compelling situation, NTISB in collaboration with E-Government Directorate may take recourse to actions/decisions currently outside the scope of this policy.
e	The policy will be reviewed from time to time in the light of actual experiences/comments of the user.

Definitions

6.   Relevant definitions are placed at Annex-A.

Network Architecture

7.   Ministry of Information Technology (MoIT)/Electronic Government Directorate(EGD) is in the process of setting up of a Federal Government Secure Intranet for providing inter-connectivity between the 42 Federal Government Divisions through a high speed Metropolitan Area Network (MAN), having a central Data Centre, which will work as the nerve centre for Federal Government and house the building blocks of this network; including a central server farm having databases of various ERP (Enterprise Resource Planning) and Citizen Service Orientated applications, Servers for customized applications for each division, Messaging & Collaboration Server, Network management Servers, Web servers, Application servers, Database servers, Core switches, Firewalls, Intrusion detection systems, Intrusion Prevention systems and Central storage facility. It will also provide central management, technical support helpdesk and monitoring of the federal Government's entire data network. The Federal Government data centre will only maintain unclassified information. Federal Government Data Centre will be responsible for provision of following IT Services:

- Email Services
- Services for hosting of ERP (Enterprise Resource Planning) applications
- Services for hosting of Citizen Service orientated applications
- Services for hosting of Internal Portals of Government Organizations
- Services for hosting of External Portals of Government Organizations

8.   The policy is essentially based on the above infrastructure to connect various Ministries and Divisions with a central data Centre to exchange unclassified information. Salient feature of the user related architecture are as under:

a   All authorized users in a Government Organization will be interconnected on a network as per detailed diagrams in Annex-C.

b   All Government Organizations will be interconnected through fiber Optic or Secure DSL/Dialup connections, which will be terminated at the Federal Government Data Centre.

c   Head of Government Organization will retain the Administrative Control of the network established in his/her domain.

d   A Network/System administrator(s) under the overall control of the controlling authority in respective Government Organizations will manage the IT Infrastructure in his/her organization as per the guideline provided at Annexes-B & C.

e   Federal Government Data Centre will be the main Service provider with the responsibilities including issue of E-mail addresses, Networking and operation of Data Centre. Services of other local ISPs will only be used where NTC services are not available.

Websites (External and Internal Portals) of Government Organizations

9.   The government web portal for federal Government of Pakistan has been created at www.pakistan.gov.pk. Web sites have been made for all Ministries/Divisions as per standard format. Guidelines given below will be followed to achieve maximum benefits while ensuring security of information:

a.   All Government Organizations will nominate a coordinator (preferably conversant with Information and communication Technology) not below the rank of a Joint Secretary, who will be assisted by System/Network(s) administrators and will be responsible for the following:

I. Ownership of the websites of respective government organization etc.

II. Updating the information on the web site of respective Government Organization on regular basis (at least twice a week) and also ensuring correctness of uploaded information.

III. Ensure that no classified information is placed on the website of Government Organization and also ensure compliance with the parameters defined in the Freedom of Information Act 2004.

IV. Coordinate provision of essential information requested by general public and answer their queries.

V. Overall administrative control of functioning of System/Network(s), e-mail services and Internet services within the Ministry/Division.

b. All Government Organizations and their related organizations should migrate to the official government portal (www.pakistan.gov.pk), unless there are compelling reasons to continue on their own web sites.

c. Government Organizations will ensure that no commercial advertisement appear on their official website.

d. Hosting/Development of websites (where not as yet initiated) will be done in consultation with Information Technology & Telecom (IT & T) Division/EGD.

e. Organizations may also register their domain names (i.e www.xyz.gov.pk) with the help of Electronic Government Directorate (EGD).

Electronic mail (E-Mail) policy guidelines

10. Following broad policy guidelines on E-Mail will be considered for the provision of email services within a Government Organization.

a. Head of a Government Organization will retain the Administrative Control of the network established in his/her domain.

b. Controlling Authority will decide as to which employee of his / her organizations should be provided with Email addresses.

c. Organizations not connected on Federal Government Intranet may register their domain names (i.e www.xyz.gov.pk) with the help of Electronic Government Directorate (EGD) and get the web based email services for its employees.

d. E-mail addresses of all users within a Government Organization will be notified by each Government Organization and published in the telephone directory issued by the Cabinet Division when notified.

e. An e-mail content guideline in line with Annex-C may be provided to users to prevent improper usage of e-mail facility.

f. Necessary software for the purpose of e-mail and Internet filtering should be in place. This will enable Network/System administrator(s) to reduce the SPAM traffic on their network(s) and will restrict the users to access any offensive material through Internet.

g. E-mail can be used for exchange of draft Documents, Exchange of general information, scheduling of internal office meetings, comments/draft minutes of meetings, circulation of office messages, other drafts etc within Government offices.

h. **To serve as legal documents, all e-mails must be maintained on the mail server for legal/audit/documentary purposes. Users will download personal copies of the e-mails on their PCs and will retain local hard copies as per procedures in vogue for record. However, the mail on the server shall be archived for a period of 180 days.**

i. Digital signatures/Digital Certificates (when issued) must be used for authentication purposes in e-mails. Supporting Server and e-mail client software should be installed to make use of PKI (Public Key Infrastructure) as and when instituted.

j. Government officials will not use Public E-mail addresses (yahoo, hotmail, etc.) for official correspondence. Government organization, where centralized E-mail systems are not provided, can use web based E-mail services provided by NTC/EGD.

Internet Services Policy Guidelines

11. Internet provides a great source of information to the users. However any computer connected to Internet is intrinsically vulnerable to eavesdropping and hacking by intruders. This therefore calls for stringent measures to be adopted to ensure security of official information and data. Following guidelines are provided on provision and use of Internet facilities to Government Organizations:

a. The Internet connection should be taken from the National Telecommunications Corporation (NTC), where available.

b. The regions in Pakistan where NTC has not established its infrastructure yet, Government offices in those regions can acquire Internet connections from their local ISPs. The choice of the local ISP should be based on the ranking of ISPs done by Pakistan Telecommunication Authority (PTA).

c. Controlling Authority will decide as to which, employees of his/her organizations should be provided with Internet access. Proper coordination is necessary between the Controlling Authority and Network/System

administrator(s) to assure the provision of Internet services to authorized users.

d. All users, within a Government Organizations authorized by Controlling Authority will be connected to the Internet through a central network gateway and properly configured firewalls (Software or Hardware Based) and Intrusion detection systems (IDS)(Software or Hardware Based). Centrally monitored/managed Anti-virus software, firewall software and IDS software should be installed on each client machine and each server of the network.

e. Organisations not connected on the Federal Government Intranet to follow the guidelines and network topologies suggested in this document.

<u>Security Policy Guidelines</u>

12. To ensure the safety/security of information and data, following guidelines are provided to be implemented on provision of Internet/ e-mail facilities in Government Organizations:

a. Head of respective Government Organizations irrespective of classification referred in this document should continue to be responsible for security of information/document/data of his/her Government Organization under the exiting rules and instructions in vogue.

b. For Work of classified/sensitive nature, separate network/environment shall be setup on case-to-case basis in the organization. This network/environment shall have no linkage with the "Internet". Head of Government Organizations will suggest deployment of such kind of Network Infrastructure only in specific departments with consultation to Cabinet Division (NTISB).

c. All Government Organizations will have properly configured Network Infrastructure and should have certified Network/System administrator(s). Coordinators nominated and Network/System administrator(s) should use OSSTMM (Open source security Testing Methodology Manual) as a standard for testing security Infrastructure of their organizations. This manual is currently downloadable at the following link: http://www.isecom.org/osstmm/

d. Only authorized licensed software to be used within government networks.

e. Strict password management policy will be followed. Passwords should not be shared and must be changed frequently as per policy to be

implemented by the Network/System Administrator(s), under the supervision of the Controlling authority.

f. All Government Organizations should notify their respective Coordinator and Network/system administrators, who should notify NTISB/EGD in case of suspected loss and disclosure of sensitive information as well as hacking or attempted hacking through internal or external network.

g. All information and data required to be placed on the web must be scrutinized by the Coordinator assisted by the Network/system administrator.

h. The use of Internet for personal e-mails, games and chatting will not be allowed on official connections.

i. No encryption software will be used by any user/organization unless authorized by the Cabinet Division (NTISB).

j. The responsibility of Physical Security of the Systems/Networks/End User Equipment shall remain with the Controlling/Coordinating Authority and the user of the equipment.

13. A list of recommended Do's and Don'ts for systems, networks and e-mail activities/usage is placed at Annex-D for implementation.

Network Security Audit

14. For Network Security audit purpose a three-layered Network Security Audit approach will be adopted.

a. First Layer. Mainly consisting of System/Network Administrators and Coordinators at Ministries / Divisions and System/Network Administrators and Security Specialists at the Federal Government Data Center to ensure correct and secure handling of systems as well as correct implementation of guidelines/instructions.

b. Second Layer. A technical audit of the System/Network Infrastructure of each Government Organization will be carried out periodically by a technical committee constituted by Cabinet Division having members as under as a second Network Security Audit layer: -

Cabinet Division (NTISB)	Permanent
IT & T Division (EGD)	Permanent
Agency Concerned	(Depending upon the concerned Organization)

The committee will carry out the implementation of above mentioned

policy guidelines with respect to following: -

- Systems/Networks Architecture.

- Vulnerabilities of licensed and customized applications.

- Implementation of instruction issued from time to time

c. <u>Third Layer.</u> A specialized/certified *Federal Network Security Audit Cell* will be established by MoIT in consultation with Cabinet Division (NTISB) comprising experts from Government officials and hired local experts (as and when required). This cell will carry out the detailed Network Security Audit(when instituted)in accordance with the guidelines/standard developed for the purpose and act as a third layer for Network Security Audit.

<u>Violation of these instruction can lead to withdrawal or suspension of right to use systems / networks privileges, and necessary disciplinary action will be taken against defaulter as per laws and regulations in vogue .</u>

Definitions

<u>Authentication</u>

Determines a user's identity, as well as determining what a user is authorized to access (view, read, write, delete, modify etc.). The most common form of authentication is user name and password, although this also provides the lowest level of security.

<u>Antivirus</u>

Refers to a program/software to help protecting a System/PC (Personal computer) from being infected with a virus.

<u>Authorized User</u>

Employees of the Federal Government who have been authorized to use e-mail and Internet facility by the Controlling Authority.

<u>Bandwidth</u>

Bandwidth is the capacity of a network to carry data/packets/information. It is normally measured in the following forms:

bps	=	bits per second
kbps	=	Kilo bits per second
Mbps	=	Mega bits per second
Gpbs	=	Giga bits per second

<u>Broadband Connections</u>

The term broadband Internet access, often shortened to "broadband Internet" or just "broadband", generically refers to last-mile Internet connections exceeding the bandwidth capabilities of standard analog modems and of ISDN connections. Broadband Internet connections are typically capable of transmitting 128 kilobits per second (kbit/s) or more.

<u>Classified Information</u>

The term includes Information related to National Security, Restricted Data, and formerly Restricted Data or any such information/data as judged by the controlling/responsible authority.

<u>Controlling Authority</u>

Head of respective Ministry/Division/Department/Autonomous Body shall be the controlling authority for the purpose of this policy.

<u>Coordinator</u>

A person who is not below the rank of a Joint Secretary and has previous knowledge of Information and communication Technology.

<u>Dial-Up Connection</u>

The most popular form of Internet connection for the home user, this is a connection from computer to a host computer (Access server in ISP) over standard telephone lines, using internal or external modems.

DSL

Digital Subscriber Line, or DSL, refers to a family of technologies that provide a digital connection over the copper wires of the local telephone network.

Dedicated Link

A dedicated link is a line, reserved exclusively for one type of communication. This is the same as a leased line or private line.

Data Center

Highly secure, fault-resistant facilities housing customer equipment that connects to telecommunications/data networks. The facilities accommodate Web servers, application servers, database servers, load balancers, email and collaboration servers, routers, core switches, firewalls, Intrusion detection systems (IDS), Intrusion prevention systems (IDP) etc. The EGD/NTC will maintain the Federal Government Data Center.

Electronic Government Directorate

An agency under the administrative control of the Ministry of IT, entrusted with the task to plan/manage/execute/monitor as well as provide guidelines to any IT related activity with the Government

E-mail

Short for electronic mail, the transmission of messages over communications networks. The messages can be entered from the keyboard or electronic files stored on disk.

Email Address

The domain-based address that is used to send electronic mail to a specified destination. For example, "Secretary@CabDiv.gov.pk" provides the following information

Secretary	indicates	Secretary (User)
Cab Div	indicates	Abbreviated/full Name of the organization
.gov.	indicates	Government Organization
.pk	indicates	A Pakistani Organization.

So, Secretary@CabDiv.gov.pk is the email address for a user, who is an employee of government of Pakistan.

Encryption

Encryption is the process of changing data into a form that can be read only by the intended receiver.

Firewall

A combination of hardware and software to protect the internal network/Intranet and IT resources from intruders or hackers who try to use the Internet/Intranet to break into those internal networks. A firewall allows only specific kinds of traffic to flow in and out of the internal network.

Government Organizations

Government Organization includes ministries/divisions/departments/Semi Autonomous Bodies.

Hacker

A person who breaks into, or attempts to break into, or use, a computer, a computer network or system without authorization, often at random, for personal amusement or gratification, and not necessarily with malicious intent.

Intranet

A network belonging to an organization or group of organizations and its sub departments, accessible only by the authorized members/systems of the organization, employees of organizations, or others with secure authentication.

Intruder

An unauthorized individual/system who attempts to hack or break into a computer system/Computer Network, or to misuse it.

Internet Connection

A communication link used to connect and exchange data to/from the Internet. It can be implemented in the form of Dial-Up, DSL connection or Fiber Optic Termination etc.

Intrusion Detection System (IDS)

A system used to identify "attempts to hack or break into a computer system" or to misuse it. IDS may monitor packets passing over the network, monitor system files, monitor log files, or set up deception systems that attempt to trap hackers.

Internet Service Provider (ISP)

A company that provides access to the Internet through an Internet connection.

Local Area Network (LAN)

A data communications network, which is geographically, limited allowing interconnection of terminals, microprocessors and computers within adjacent buildings (normally within radius of 1KM).

License Software

A Software, which grants a special permission of being used under specified condition of copyright and other laws by the manufacturer.

National Telecommunication Corporation (NTC)

A government owned telecommunication organization to provide telecommunication services to its designated customers, which includes Federal and Provincial Governments and their departments.

Pakistan Telecommunication Authority (PTA)

PTA is a telecommunication regulatory body, which regulates the establishment, operations and maintenance of telecommunication services. It also promotes and protects the interests of telecommunication service providers and users.

Password

A unique string of characters that a user types as an identification code to restrict access to computers and sensitive files.

Server

A computer or device on a network that manages network resources. For example, a file server is a computer dedicated to storing files, a print server is a computer that manages one or more printers and an application server is a server which hosts applications.

Stand-alone PC

Refers to a computer that is self-contained, one that does not require any other devices to function and also does not connected to any type of network.

Spam

An inappropriate attempt to use a mailing list, or other networked communications facility as if it was a broadcast medium by sending the same message to a large number of people who didn't ask for it. Mass junk e-mail.

Virtual Private Network (VPN)

Usually refers to a network in which some of the parts are connected using the public Internet, but the data sent across the Internet is encrypted, so the entire network is "virtually" private. A typical example would be a company network where there are two offices in different cities. Using the Internet the two offices merge their networks into one network, but encrypt traffic that uses the Internet link.

Web Portal

Commonly referred to as simply a portal, a Web site or collection of websites or service that offers a broad array of resources and services. The address of Web Portal of Government of Pakistan is www.Pakistan.gov.pk. It is hosted at NTC and is being maintained by EGD. Commonly there are two kinds of portals for large organizations. The first one is an internal portal of an organization, which servers the employees of the organization and its sub departments for information, news and applications available. Second one is an external portal, which extracts information from the internal portal or databases of organization automatically and displays it for public information.

DEPARTMENTAL SECURITY MANUAL

The Office's internal network introduces new resources and new services through Local Area Network and Internet connectivity. This connectivity not only results in new capabilities, but also in new risks and threats. This document formally defines a departmental security policy regarding Network resource usage, rights and restrictions. All network users are expected to be familiar with and to comply with this policy.

The scope of this policy includes the following information:

    a. Authorized Software

    b. Backup and Recovery

    c. File and Print Services

    d. Hardware Rights and Restrictions

    e. Internet Access

    f. Mail Management

    g. Network Protection

    h. Network/PC Usage

    i. Non-Organization Personnel

    j. Password Policy

    k. Removal of Privileges

    l. Virus Protection

    m. Help Desk

Authorized Software

The Network/System Administrator(s) will install only the Authorized Software on the departmental machines (PC/Laptop). No individual/user will install any Software on their own. The user will contact the Network/System Administrator(s) to install an authorized software that have direct relevance to the office work. If any additional software needs to be installed, the user would take prior approval of Coordinator on a prescribed form available with Network/System Administrator(s).

Any software required by users should have security cleared from the Network Administrator(s).

Backup and Recovery

Backups will be taken weekly. Tape cartridges or other removable media may be used for data backup and the following strategy would be used for backing up data:

- Full backup of all servers, folders and emails would be taken on two tape cartridges. One of which would be placed in the server room and the other one would be placed in a different physical location. Doing this we will achieve two goals, first if server crashes then one can recover all data from the tape cartridge placed in server room and second if that tape cartridge fails or server room faces a natural disaster then one can recover the data from the tape cartridge which was placed in the different physical location.

- The remaining cartridges may be used for incremental backups.

The backup may be taken of the following servers, user's folders and their emails:

- Database Server (Database)

- Network Shared Directories

- Email Server (Mailboxes)

- File and Print Server (Main Server)

Hardware Rights and Restrictions

Modem of every PC or laptop should be automatically disabled, whenever they will join the domain of office network. The use of other peripheral devices (CD drives, Writable CD drives, Floppy drive, USB drives, USB ports etc.) should be minimized as these are also the potential sources of viruses, Trojans, leakage of information etc.

Specific Auditing, which monitors user interaction with the key system resources, should be enabled on the hard drives of laptops, which will help administrators monitor any improper use of the laptops.

Internet Access

The following Standard Internet services will be provided to users after the prior approval of Controlling Authority:

- E-mail -- Send/receive E-mail messages to/from the Internet (with or without document attachments).

- Navigation -- WWW services as necessary for official purposes.

To further improve network security and to optimize Internet access, the following guidelines should be adhered by the users:

- A list of prohibited websites will be kept at server level and such sites will be blocked using the proxy server software. This list of prohibited web sites will be drawn up in consultation with the coordinator.

- Network Administrator(s) should monitor Internet downloading. Proxy servers should be configured in such way that Network/system administrator(s) should be able to report the following two items:
  - Bandwidth used by each user within a month.
  - Names of all the sites visited by each user within a month.

  Proper logs of the above two mentioned items should be maintained by the network administrator(s).
- Networked workstations should not be connected to separate analog lines or modems i.e. direct Dial-up connection is not allowed to any user for access to the internet while sitting within the organization.
- Where necessary with the approval of NTISB, Remote users can dial in to the access server using VPN client software.

Mail Management

The email addresses should be created keeping in mind a standard naming convention.

Naming convention for email addresses should be the initial of first name plus the last name. Organization = Domain name of Organization.

But in case of same first alphabet of first name and same last name, first two alphabets of first name may be used to avoid any confusion.

The top and middle management would maintain dual E-mail accounts. One with their designation and the other with the initial of their first name plus the last name.

Users should consider the following to better manage e-mail activities:
- Employees should compress large size files before attaching with the email. This will help to optimize the bandwidth.
- Employees should delete items from their inbox and outbox when they are no longer needed. If a mail item needs to be retained it should be moved to an archive folder, a disk, or be printed or deleted. Unsolicited mail should be deleted immediately.
- Employees should check their e-mail with a frequency appropriate to their jobs. Employees who will be absent for more than one day should make arrangements for a supervisor or co-worker to check for messages that need attention, OR, an automatic reply message may be configured with the help of Network/system administrator.
- It is possible to receive a virus when receiving e-mail, and some viruses are embedded in attachments. If you receive a suspicious e-mail, do not open it, but instead contact the Network/System Administrator.

- Some computer features increase e-mail traffic, and employees should strive to keep message and attachment sizes as small as possible. Avoid the use of graphics in auto-signatures or other parts of the message or attachments. Use of stationary should be avoided, as well as moving graphics and/or audio objects as they consume more disk space, network bandwidth, and detract from the message content.
- Users may not discuss their opinions on religious/sectarian, or political matters. Users may not use email to propagate indiscipline in office matters. Users may not use email for purposes of disrepute/ill repute of any individual or organization. Users may only use proper official language in their emails, and refrain from using words in other languages transcribed in English.
- It is also advised that users should use a standard email disclaimer, with each outgoing email. Email disclaimer can be standardized for every organization with the help of Network/system administrator and head of organization.

Network / PC Usage

The users should follow the following practices:

- Users must use password protected screen savers to avoid misuse of their PCs by unauthorized personnel. Users leaving their computers unattended for more than 15 minutes should consider logging off the network.
- Users must log off the network at the end of each day and power off their workstations.
- Users are responsible for the security of their LAN user ID and Password.
- Users are accountable for any actions that are taken with their user ID and Password.

The Internet, Intranet and e-mail access may not be used at any time for:

- Downloading, installing, or running security programs or utilities which reveal weaknesses in the security of the network unless a job specifically requires it.
- Use of computers and User IDs for which there is no authorization, or use of User IDs for purposes outside of those for which they have been issued.
- Attempting to modify, install or remove computer equipment, software, or peripherals without proper authorization. This includes installing any software not related to official work requirements.
- Accessing computers, computer software, computer data information, or networks without proper authorization. Circumventing or attempting to circumvent logon procedures, and security regulations, or exceeding the system's capacity limits by downloading excessive materials.
- The use of computing facilities, User IDs, or computer data for purposes other than those for which they are intended or authorized.

- Breaking into another user's e-mailbox, or unauthorized personnel reading someone else's e-mail without permission.
- Sending fraudulent electronic transmissions, including but not limited to statements intended to mislead the receiver and are known to be untrue, fraudulent requests for confidential information, fraudulent submission of electronic purchase requisitions or journal vouchers, or fraudulent electronic authorization of purchase requisitions or journal vouchers.
- Violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization.
- Encroaching on or disrupting others' use of the shared network resources by creating unnecessary network traffic (for example, playing games or sending excessive messages); excessive use of using memory, bandwidth and disk space resources; interfering with connectivity to the network; modifying system facilities, operating systems, or disk partitions without authorization; attempting to crash or tie up a computer; damaging or vandalizing computing facilities, equipment, software, or computer files).
- Disclosing or removing proprietary information, software, printed output or magnetic media without the explicit permission of the owner.
- Reading other users' data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission. This does not prohibit Controlling Authority having access to users' computers.

Network Protection

Internet connectivity presents the organization with new risks that must be addressed to safeguard the facility's vital information assets. Network administrator(s) will ensure that properly configured Firewall and filtering systems are in place to technically support the access requirements defined by this policy. In-bound traffic from the Internet will not be permitted except for E-mail and access to public mail servers.

Hardware or software firewall should be installed and configured to protect the network from unauthorized access and intrusion into the Office's local area network from the Internet. All electronic traffic would route through this firewall that would be centrally monitored. Access to specific websites and ports would be managed through this.

Non-Organization Personnel

External clients or non-organization personnel are not permitted access to organization internal network resources unless specifically approved in advance by the Controlling Authority.

<u>Password Guidelines</u>

The following steps will be been taken by the users to improve password security:

- Users are required to change their password with in 30 days. If a user does not change his/her password with in 30 days, he/she will be automatically prompted for the change of password.

- In addition, passwords must be chosen by the users which are difficult to guess. This means that passwords must not be related to one's job or personal life. For example, a car license plate number, a spouse's name, or fragments of an address must not be used. This also means passwords must not be a word found in the dictionary or some other part of speech. For example, proper names, places, technical terms, and slang must not be used. Password control software will be used to prevent users from selecting easily-guessed passwords. A good password may be a mixture of alphabets in upper & lower case along with numbers.

<u>Removal of Privileges</u>

Internet access will be discontinued upon termination of employee, completion of contract, end of service of non-employee or disciplinary action arising from violation of this policy. In the case of a change in job functions and/or transfer the original access code will be discontinued and reissued only if necessary and a new request for access is approved by the Controlling Authority.

<u>Virus Protection</u>

The Network should be protected from viruses by using industry standard Antivirus software (Corporate Editions). This should be scheduled to automatically update the clients and servers after daily centralized downloading of latest virus definition files (DAT file) from the Internet at night.
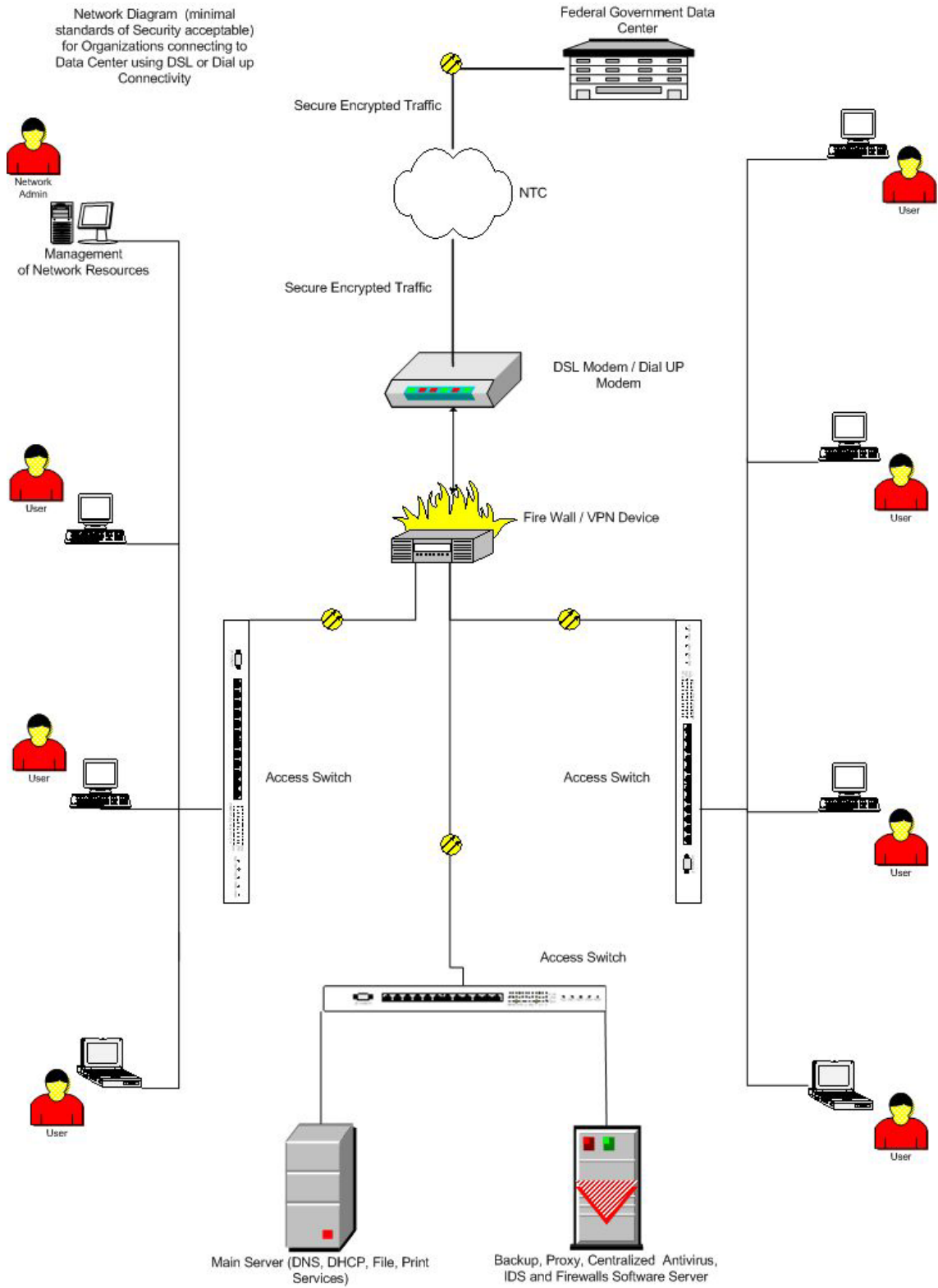
<u>Help Desk</u>

Help Desk should be available for the user support. Network/System administrators sitting at the help desk should be facilitated with internal phone facilities.

Network Diagrams
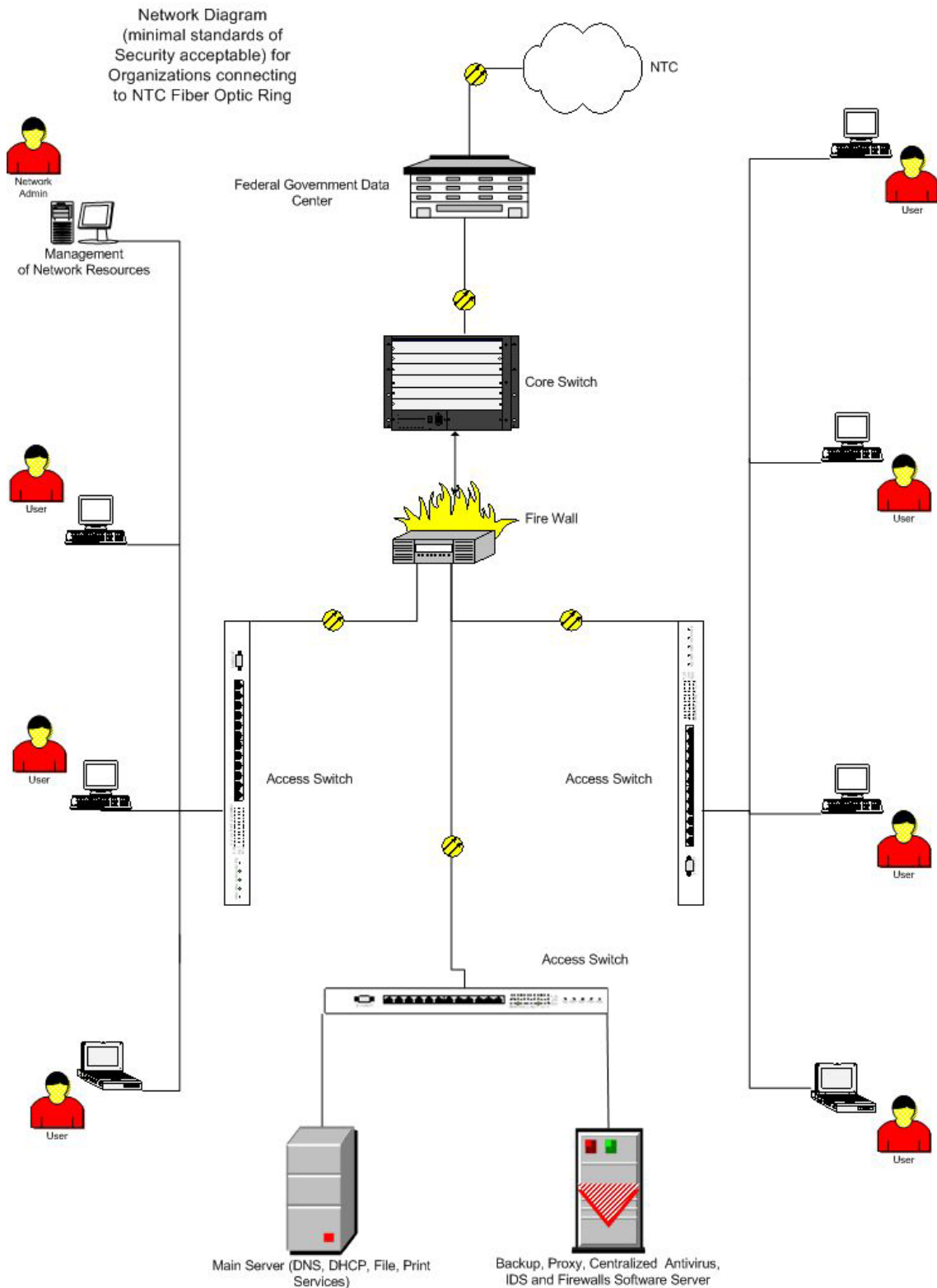
Network Diagram
(minimal standards of
Security acceptable) for
Organizations connecting
to NTC Fiber Optic Ring

NTC

Network
Admin

Management
of Network Resources

Federal Government Data
Center

User

Core Switch

Fire Wall

User

User

Access Switch

Access Switch

User

User

Access Switch

User

User

Main Server (DNS, DHCP, File, Print
Services)

Backup, Proxy, Centralized Antivirus,
IDS and Firewalls Software Server
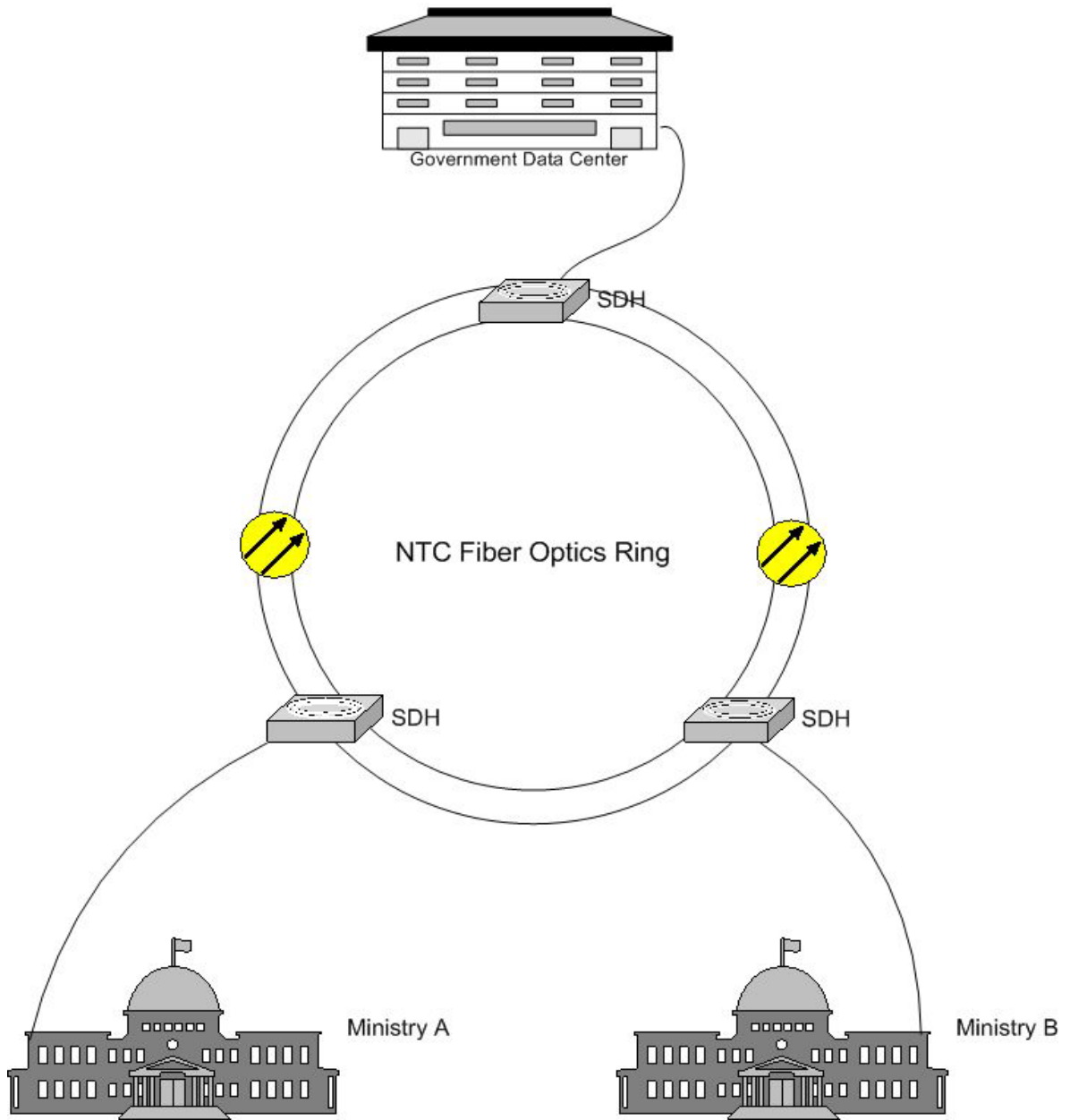
Network Diagram (minimal standards of Security acceptable) for Organizations connecting to Data Center using DSL or Dial up Connectivity

Federal Government Data Center

Secure Encrypted Traffic

NTC

Network Admin

Management of Network Resources

Secure Encrypted Traffic

DSL Modem / Dial UP Modem

User

User

Fire Wall / VPN Device

User

Access Switch

Access Switch

User

User

Access Switch

User

User

Main Server (DNS, DHCP, File, Print Services)

Backup, Proxy, Centralized Antivirus, IDS and Firewalls Software Server

21

Federal Government Intranet

Government Data Center

SDH

NTC Fiber Optics Ring

SDH

SDH

Ministry A

Ministry B

RECOMMENDED DO'S AND DON'T'S

FOR SYSTEMs, NETWORKs AND E-MAIL ACTIVITIES

Do's

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; user level passwords should be changed every month.

2. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 5 minutes or less, or by logging-off, when the host will be unattended.

3. Information contained on portable computers' laptops is especially vulnerable, special care should be exercised.

4. Postings by employee from one organization to other, email address to old organization should contain a disclaimer stating that the opinions expressed are strictly his/her own after leaving the official duties and not necessarily those of official unless posting is in the course of official duties.

5. All hosts used by the employee that are connected to the Federal Internet/Intranet, shall be continually executing approved virus-scanning software with a current virus database.

6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Don'ts

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). The lists below are by no means exhaustive, but attempt to provide a framework for activities, which fall into the category of unacceptable use. Under no circumstances a user of Federal Internet/Intranet is authorized to engage in any activity that is illegal under, Federal or International law while utilizing Federal owned resources. The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or state protected by copyright, official secret act, or similar laws or regulations.
2. Unauthorized copying of official correspondence material including, digitization and distribution of photographs/ official correspondence or other copyrighted sources, , and the installation of any copyrighted software for which the end user does not have an active license is strictly prohibited.
3. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
4. Revealing your account password to others or allowing use of your account by others. *This includes family and other household members when work is being done at home.*
5. Using a Federal computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
6. Making fraudulent offers of products, items, or services originating from any Federal account.
7. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
8. Port scanning or security scanning is expressly prohibited.
9. Executing any form of network monitoring which will intercept data not intended for the employee's host.
10. Circumventing user authentication or security of any host, network or account.
11. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
12. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet.
13. Providing information about, or lists of, organization.
14. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email Spam).

15. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

16. Unauthorized use, or forging, of email header information.

17. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

18. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

19. Use of unsolicited e-mail originating from within Federal Data Networks of other Internet/Intranet service providers on behalf of, or to advertise, any service hosted by Federal Data Networks or connected via Federal Data Networks.

20. Posting the same or similar non-official business related messages to large numbers of Usenet newsgroups (newsgroup Spam).