PREFACE

The e-District project, a Mission Mode Project under National e-Governance Plan, is being implemented in the State of Assam covering all the districts in a phased manner. The main objective of the project is to deliver the various public services dealt by the district administration to the citizen electronically through various delivery channels like Common Service Centres (CSCs) and Public Facilitation Centres (PFCs) in an efficient and time bound manner.

The e-District project implemented in the district level has got various components such as site development, deployment of IT infrastructure, providing connectivity through ASWAN, application designing, data digitization, capacity building of staff and CSC operators and orientation workshop etc. to create an eco-system for electronic processing and delivery of services in electronic mode.

The success of the e-District project, like any other e-Governance project, largely depends on the ownership and participation in the project by the staff and employees throughout hierarchy.

Keeping in view the changes to be brought with introduction of new system of working and driving the project in line with the overall spirit of service orientation, lot of thrust has been given on the Change Management and Training of the employee/staff in the districts.

The training being the core of the entire Change Management initiative, necessary training plan have been devised for imparting necessary training and handholding throughout the hierarchy. This Specialized IT course for staff and employees of the district administration has been designed keeping in mind that they become aware of the entire electronic service delivery eco-system.

This course covers various aspects like concept of basic e-Governance, legal and
statutory provision of the India IT Act, digital signature, NeGP programs and its components, e-District program and other relevant details.

It is hoped that the course content would be useful for the participants
# TABLE OF CONTENTS

## Chapter 1: Good Governance

**GOOD GOVERNANCE** .......................................................................................................................2

- EFFECTIVENESS AND EFFICIENCY .................................................................................................2
- RESPONSIVENESS ..............................................................................................................................2
- CONSENSUS ORIENTED .......................................................................................................................3
- EQUITY AND INCLUSIVENESS ...........................................................................................................3
- RULE OF LAW .................................................................................................................................3

**E-GOVERNANCE** ............................................................................................................................3

- WHY TO INTRODUCE E-GOVERNANCE? .........................................................................................4

## Chapter 2: Introduction to IT Act 2000/2008

**INTRODUCTION:** THE PURPOSE OF ENACTING IT ACT, 2000 ........................................................9

**AIMS AND OBJECTIVES OF IT ACT 2000** ....................................................................................10

- A BRIEF INTRODUCTION TO IT ACT 2000/ 2008 (AMENDED) .....................................................11
- THE IT ACT 2000 AS AMENDED BY THE IT (AMENDMENT) ACT, 2008 ........................................11

- CHAPTER I: PRELIMINARY .................................................................................................................11
- CHAPTER II: DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE ..............................................12
- CHAPTER III: ELECTRONIC GOVERNANCE ......................................................................................12
- CHAPTER IV: ATTRIBUTION, ACKNOWLEDGMENT AND DISPATCH OF ELECTRONIC RECORDS ....13
- CHAPTER V: SECURE ELECTRONIC RECORDS AND SECURE ELECTRONIC SIGNATURES ..........13
- CHAPTER VI: REGULATION OF CERTIFYING AUTHORITIES ..........................................................13
- CHAPTER VII: ELECTRONIC SIGNATURE CERTIFICATES ...............................................................14
- CHAPTER VIII: DUTIES OF SUBSCRIBERS .......................................................................................14
- CHAPTER IX: PENALTIES, COMPENSATION AND ADJUDICATION .............................................15
- CHAPTER X: THE CYBER APPELLATE TRIBUNAL ...........................................................................15
CHAPTER XI: OFFENCES .................................................................................................................. 16
CHAPTER XII: INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES ........................................ 18
CHAPTER XII-A: EXAMINER OF ELECTRONIC EVIDENCE ................................................................. 18
CHAPTER XIII: MISCELLANEOUS ..................................................................................................... 19

IT ACT 2008 (AMENDED) ..............................................................................................................19

Chapter 3 IT Act and Provisions of Electronic Delivery of Government Services

THE ELECTRONIC DELIVERY OF SERVICES ..............................................................................22
Need for the Electronic Delivery of Services Rules .................................................................... 22
Benefits of the Electronic Delivery of Services Rules ................................................................. 25
Key Features of Other State Rules .................................................................................................26

Chapter 4: Program and Infrastructure of Delivery of e-Services

NATIONAL E-GOVERNANCE PLAN (NEGP) ............................................................................ 29
Implementation Strategy, Approach and Methodology of NEGP ........................................... 29
Projects Identified Under NEGP .................................................................................................. 32
Institutional Framework for Implementation .............................................................................. 33
NEGP Core Infrastructure ............................................................................................................. 34

STATE WIDE AREA NETWORK (SWAN) .................................................................................. 34
Implementation Model .................................................................................................................. 35
Assam State Wide Area Network (ASWAN) Structure ............................................................. 36
SWAN for Department: Strategy .....................................................................................................36
State Data Centre (SDC) ................................................................................................................ 37
Assam State Data Center .............................................................................................................. 38
**SSDG & STATE PORTAL (STATE SERVICE DELIVERY GATEWAY AND STATE POTAL) ..........39**

- OBJECTIVES OF SSDG ............................................................................................................. 40
- STATE PORTAL......................................................................................................................... 41
- SP-SSDG PROJECT IN ASSAM.............................................................................................. 41
- SSDG INTEGRATION WITH MMPS....................................................................................... 42

**NSDG .................................................................................................................................. 43**

**COMMON SERVICES CENTRES (CSC) ........................................................................... 45**

- ARUNODOY COMMON SERVICES CENTERS (CSC) PROJECT ........................................ 47

**CLOUD COMPUTING ........................................................................................................... 50**

- ARCHITECTURAL VISION OF GI CLOUD ............................................................................ 50

**INDIA’S E-GOVERNANCE STANDARDS ........................................................................ 51**

- OBJECTIVES OF E-GOVERNANCE STANDARDS ................................................................ 52

**OPEN STANDARD ................................................................................................................. 54**

- E-AUTHENTICATION OR E-PRAMAAN ............................................................................. 55
- BENEFITS OF E-AUTHENTICATION ..................................................................................... 55
- OVERVIEW OF E-AUTHENTICATION MECHANISMS .......................................................... 56
- LEVELS OF AUTHENTICATION ASSURANCE ..................................................................... 56

**M-GOVERNANCE ................................................................................................................ 58**

- MOBILE SEVA ....................................................................................................................... 58

**E-MAIL SYSTEM .................................................................................................................... 60**

- E-MAIL VIEWS ....................................................................................................................... 60
- READ NEW EMAIL ................................................................................................................... 61
- SEND EMAIL ............................................................................................................................ 61
- INSTRUCTIONS FOR NEW E-MAIL USER REGISTRATION .............................................. 62
- LIMITS AT MAIL GATEWAYS ............................................................................................... 63
- LIMITS FOR MAIL CLIENTS ................................................................................................... 63
Chapter 5: e-District Project

THE E-DISTRICT PROJECT ........................................................................................................ 68

OBJECTIVE OF THE E-DISTRICT PROJECT .............................................................................. 68

SERVICE TYPE AS DEFINED IN THE NATIONAL ROLL OUT .................................................. 70
  TYPE 1 SERVICES ....................................................................................................................... 70
  TYPE 2 SERVICES ....................................................................................................................... 71
  TYPE 3 SERVICES ....................................................................................................................... 71
  QUALITY OF SERVICE .............................................................................................................. 71
  SERVICE LEVEL ......................................................................................................................... 71

E-DISTRICT DEPLOYMENT FRAMEWORK .............................................................................. 72
  FUNCTIONAL ARCHITECTURE ................................................................................................... 73
  INSTITUTIONAL FRAMEWORK ENVISAGED ........................................................................... 74

FRAMEWORK OF DEGS ........................................................................................................... 74
  APPROVAL OF CABINET ............................................................................................................ 74
  OBJECTIVES OF THE DEGS ...................................................................................................... 75
  GOVERNING BODY .................................................................................................................... 76
  FUND PROVISIONS .................................................................................................................... 76
  CAPACITY BUILDING .................................................................................................................. 76

E-DISTRICT PROJECT IN ASSAM ........................................................................................... 77
  SERVICES OFFERED THROUGH ASSAM E-DISTRICT PROJECT .......................................... 77
  SOME KEY LEARNING OF THE PILOT .................................................................................... 78
  PROPOSED SERVICE DELIVERY MECHANISM ...................................................................... 79
  PROJECT IMPLEMENTATION ..................................................................................................... 80
Chapter 6: Introduction to IT Security Policy

CYBER CRIMES: LAW AND PRACTICE.................................................................84
IT SECURITY POLICY.........................................................................................86
THE INDIAN CYBER SPACE ...........................................................................86
THE INFORMATION TECHNOLOGY (IT) ACT 2000.........................................87
NATIONAL CYBER SECURITY POLICY 2013...............................................89
INFORMATION SECURITY POLICY FOR ORGANIZATIONS .......................90

Chapter 7: The UIDAI Project

THE UNIQUE IDENTIFICATION (UIDAI) PROJECT........................................94
WHAT IS AADHAAR?.......................................................................................96
   EVERY INDIVIDUAL IS UNIQUE.....................................................................97
       BENEFITS OF HAVING A UNIQUE IDENTITY........................................97
   THE FEATURES OF UID OR AADHAAR......................................................99
       BENEFITS OF AADHAAR FOR RESIDENTS.........................................100
       BENEFITS OF AADHAAR FOR GOVERNMENT....................................100
   USE OF AADHAAR....................................................................................101
E-AADHAAR..................................................................................................102
Chapter 1

Good Governance

Chapter Objectives:

Good governance means that processes and institutions produce results that meet the needs of society while making the best use of resources at their disposal. Good governance appears alongside such terms such as democracy, civil society, participation, human rights and sustainable development. It has been closely associated with the public sector reform since last decade. This chapter covers major concepts of good governance as a whole.

Chapter in a Nutshell:

GOOD GOVERNANCE

- Effectiveness and Efficiency
- Responsiveness
- Consensus Oriented
- Equity and Inclusiveness
- Rule of Law

E-GOVERNANCE

- Why to introduce E-Governance?
Good Governance

Good governance is a concept that has come into regular use in political science, public administration and, more particularly, development management. It appears alongside such terms such as democracy, civil society, participation, human rights and sustainable development. In the last decade, it has been closely associated with the public sector reform.

Good governance has 8 major characteristics. It is participatory, consensus oriented, accountable, transparent, responsive, effective and efficient, equitable and inclusive and follows the rule of law. It assures that corruption is minimized, the views of minorities are taken into account and that the voices of the most vulnerable in society are heard in decision-making (OECD, 2001).

Participation by both men and women is a key cornerstone of good governance. Participation could be either direct or through legitimate intermediate institutions or representatives. Participation needs to be informed and organized. This means freedom of association and expression on the one hand and an organized civil society on the other hand.

Transparency means that decisions taken and their enforcement are done in a manner that follows rules and regulations. It also means that information is freely available and directly accessible to those who will be affected by such decisions and their enforcement. It also means that enough information is provided and that it is provided in easily understandable forms and media.

Effectiveness and Efficiency

Good governance means that processes and institutions produce results that meet the needs of society while making the best use of resources at their disposal. The concept of efficiency in the context of good governance also covers the sustainable use of natural resources and the protection of the environment.

Responsiveness

Good governance requires that institutions and processes try to serve all stakeholders within a reasonable time frame.

Accountability is a key requirement of good governance. Not only governmental institutions but also the private sector and civil society organizations must be accountable to the public and to their institutional stakeholders. Who is accountable to whom depending on whether decisions or actions taken are internal or external to an organization or institution. In general an organization or an institution is accountable to those who will be affected by its decisions or actions. Accountability cannot be enforced without transparency and the rule of law.
Consensus Oriented

There are several actors and as many viewpoints in a given society. Good governance requires mediation of the different interests in society to reach a broad consensus in society on what is in the best interest of the whole community and how this can be achieved. It also requires a broad and long-term perspective on what is needed for sustainable human development and how to achieve the goals of such development. This can only result from an understanding of the historical, cultural and social contexts of a given society or community.

Equity and Inclusiveness

A society’s wellbeing depends on ensuring that all its members feel that they have a stake in it and do not feel excluded from the mainstream of society. This requires all groups, but particularly the most vulnerable, have opportunities to improve or maintain their wellbeing.

Rule of Law

Good governance requires fair legal frameworks that are enforced impartially. It also requires full protection of human rights, particularly those of minorities. Impartial enforcement of laws requires an independent judiciary and an impartial and incorruptible police force.

e-Governance

e-Governance is use of information and communication technologies by the Governments with the aim of improving information and service delivery, encouraging citizen participation in the decision-making process and making government more accountable, transparent and effective.

Goals of e-governance:

- Improve the internal organisational processes of governments
- Provide better information and service delivery
- Increase government transparency in order to reduce corruption
- Reinforce political credibility and accountability

Promote democratic practices through public participation and consultation. e-Governance is generally considered as a wider concept than e-government, since it can bring about a change in the way how citizens relate to governments and to each other. Its objective is to engage, enable and empower the citizen.
Why to introduce e-Governance?

The purpose of implementing e-governance is to enhance good governance. Good governance is generally characterized by participation, transparency and accountability. The recent advances in communication technologies and the Internet provide opportunities to transform the relationship between governments and citizens in a new way, thus contributing to the achievement of good governance goals. The use of information technology can increase the broad involvement of citizens in the process of governance at all levels by providing the possibility of on-line discussion groups and by enhancing the rapid development and effectiveness of pressure groups. Advantages for the government involve that the government may provide better service in terms of time, making governance more efficient and more effective. In addition, the transaction costs can be lowered and government services become more accessible.

The fields of implementation of e-governance are:

- **e-Administration**: refers to improving of government processes and of the internal workings of the public sector with new ICT-executed information processes.

- **e-Services**: refers to improved delivery of public services to citizens. Some examples of interactive services are: requests for public documents, requests for legal documents and certificates, issuing permits and licenses.

- **e-Democracy**: implies greater and more active citizen participation and involvement enabled by ICTs in the decision-making process.

Chapter Summary

- Good governance means that processes and institutions produce results that meet the needs of society while making the best use of resources at their disposal.

- Good governance requires that institutions and processes try to serve all stakeholders within a reasonable timeframe.

- Good governance requires fair legal frameworks that are enforced impartially.

- The purpose of implementing e-governance is to enhance good governance. Good governance is generally characterized by participation, transparency and accountability.
Chapter 1: Good Governance

**Exercises**

1. What do you mean by Good Governance?
2. Explain importance of Good Governance.
3. Why introduce e-Governance?
4. Explain the fields which e-Governance implement.
5. Describe Goals of e-Governance.
Chapter 2

Introduction to IT Act 2000/2008

Chapter Objectives:

With the increased use of Computers as a basic tool of Communication, Information Processing, Information Storage, Physical Devices Control etc., a new cyber world has come into existence. In order to regulate, monitor and control the electronics transaction taking place in a cyber space and to provide necessary legal validity and ensure security of such transaction, many countries across the world has enacted specific law for their respective countries to govern the cyber space. The laws are being amended from time to time with change of technology and other related matters. India also has enacted its own Information Technology Act in 2000. This chapter gives an overview to the Indian IT Act 2000/2008.

Chapter in a Nutshell:

AN INTRODUCTION TO INDIAN IT ACT 2000/2008

THE PURPOSE OF ENACTING IT ACT, 2000

AIMS AND OBJECTIVES OF IT ACT 2000

IT ACT 2000 & IT ACT (AMENDED)
THE IT ACT 2000 AS AMENDED BY THE IT (AMENDMENT) ACT, 2008

Chapter i: Preliminary
Chapter ii: Digital Signature and Electronic Signature
Chapter iii: Electronic Governance
Chapter iv: Attribution, Acknowledgment and Dispatch of Electronic Records
Chapter v: Secure Electronic Records and Secure Electronic Signatures
Chapter vi: Regulation of Certifying Authorities
Chapter vii: Electronic Signature Certificates
Chapter viii: Duties of Subscribers
Chapter ix: Penalties, Compensation and Adjudication
Chapter 2: Introduction to Indian IT Act 2000/2008

Chapter x: The Cyber Appellate Tribunal
Chapter xi: Offences
Chapter xii: Intermediaries not to be liable in certain cases
Chapter xii-a: Examiner of Electronic Evidence
Chapter xiii: Miscellaneous
Introduction: The Purpose of Enacting IT Act, 2000

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

Model Law on e-Commerce was adopted in 1996 by United Nations Commission on International Trade and Law (UNCITRAL). It was then adopted by the General Assembly of the United Nations by passing a resolution on 31st January, 1997. In continuation to the same, India was also a signatory to this Model Law and had to revise its national laws as per the said model law. Therefore, India enacted the Information Technology Act, 2000 and it was amended by the Information Technology (Amendment) Act, 2008.

Following are the main national and international reasons for the enactment of the IT Act, 2000:

- Increasing use of ICTs in conducting business transactions and entering into contracts, because it was easier, faster and cheaper to store, transact and communicate electronic information than the traditional paper documents.

- Business people were aware of these advantages but were reluctant to interact electronically because there was no legal protection under the existing laws.

- International trade through electronic means was growing tremendously and many countries had switched over from traditional paper based commerce to e-commerce.

- The United Nations Commission on International Trade Law (UNCITRAL) had adopted a Model Law on Electronic Commerce in 1996, so as to bring uniformity in laws governing e-commerce across the globe.

- India, being a signatory to UNCITRAL, had to revise its national laws as per
Because the World Trade Organization (WTO) was also likely to conduct its transactions only in electronic medium in future.

**Aims and Objectives of IT Act 2000**

Following were the main aims and objectives of the IT Act, 2000:

- To suitably amend existing laws in India to facilitate e-commerce.
- To provide legal recognition of electronic records and digital signatures.
- To provide legal recognition to the transactions carried out by means of Electronic Data Interchange (EDI) and other means of electronic communication.
- To provide legal recognition to business contacts and creation of rights and obligations through electronic media.
- To establish a regulatory body to supervise the certifying authorities issuing digital signature certificates.
- To create civil and criminal liabilities for contravention of the provisions of the Act and to prevent misuse of the e-business transactions.
- To facilitate e-Governance and to encourage the use and acceptance of electronic records and digital signatures in government offices and agencies. This would also make the citizen-government interaction more hassle free.
- To make consequential amendments in the Indian Penal Code, 1860 and the Indian Evidence Act, 1872 to provide for necessary changes in the various provisions which deal with offences relating to documents and paper based transactions.
- To amend the Reserve Bank of India Act, 1934 so as to facilitate electronic fund transfers between the financial institutions.
- To amend the Banker’s Books Evidence Act, 1891 so as to give legal sanctity for books of accounts maintained in the electronic form by the banks.
The IT Act 2000 as amended by the IT (Amendment) Act, 2008

The Indian IT Act 2000 as amended by The IT (Amendment) Act, 2008 contains 13 Chapters named as follows:

- Chapter i: Preliminary
- Chapter ii: Digital Signature and Electronic Signature
- Chapter iii: Electronic Governance
- Chapter iv: Attribution, Acknowledgment and Dispatch of Electronic Records
- Chapter v: Secure Electronic Records and Secure Electronic Signatures
- Chapter vi: Regulation of Certifying Authorities
- Chapter vii: Electronic Signature Certificates
- Chapter viii: Duties of Subscribers
- Chapter ix: Penalties, Compensation and Adjudication
- Chapter x: The Cyber Appellate Tribunal
- Chapter xi: Offences
- Chapter xii: Intermediaries not to be liable in certain cases
- Chapter xii-a: Examiner of Electronic Evidence
- Chapter xiii: Miscellaneous

Following are the description of each provision and its sections of Indian IT Act 2000 as amended by The IT (Amendment) Act, 2008:

**Chapter i: Preliminary**

The preliminary provision covers the following sections:

1. Short Title, Extent, Commencement and Application
2. Definitions: Covers definitions of major terms used in the IT Act
Chapter ii: Digital Signature and Electronic Signature

Digital signature is a secure method of binding the identity of the signer with electronic record or message. This method uses a public key crypto system commonly known as 'asymmetric crypto system' to generate digital signature. Digital signature is used to ‘authentication of any electronic record by a subscriber by means of an electronic method or procedure’. The Digital Signature and Electronic Signature provision covers the following sections:

3. Authentication of Electronic Records
   3A. Electronic Signature

Chapter iii: Electronic Governance

In today’s world, we have various new concepts like e-contract, e-communication, e-transaction, e-Governance and so on. Computers, internet and ICTs have various advantages and had brought tremendous change in our lives.

e-Governance is the application of ICTs to the processes of government functioning so as to have simple, accountable, speedy, responsive and transparent governance. Further, the World Bank defines e-Governance as the use of information and communication technologies by government agencies to transform relations with citizens, business and other arms of the government. It involves information technology enabled initiatives that are used for improving:

a. The interaction between government and citizens or government and business commonly known as e-services;

b. The internal government operations commonly known as e-administration; and

c. External interaction among the members of society commonly known as e-society.

Electronic Governance provision of IT Act covers the following sections:

4. Legal recognition of Electronic Records
5. Legal recognition of Electronic Signature
6. Use of Electronic Records and Electronic Signature in Government and its agencies
   6A. Delivery of Services by Service Provider
7. Retention of Electronic Records
7A. Audit of Documents etc. in Electronic form

8. Publication of rules, regulation, etc., in Electronic Gazette

9. Sections 6, 7 and 8 Not to Confer Right to insist document should be accepted in electronic form

10. Power to Make Rules by Central Government in respect of Electronic Signature

10A. Validity of contracts formed through electronic means.

Chapter iv: Attribution, Acknowledgment and Dispatch of Electronic Records

e-Contract means contract formed in electronic form. Further, e-contract is a part and parcel of e-commerce. Under the IT Act, 2000 earlier there was no provision relating to e-contract, but the IT (Amendment) Act, 2008 has inserted Section 10A which confers the validity on contracts formed in e-form. This provision defines different Attribution, Acknowledgment and Dispatch of Electronic Records. Following are the sections covered under this provision:

11. Attribution of Electronic Records
12. Acknowledgement of Receipt
13. Time and place of dispatch and receipt of electronic record

Chapter v: Secure Electronic Records and Secure Electronic Signatures

This provision defines different ways to secure Electronic Records and Secure Electronic Signatures. Following are the sections covered under this provision:

14. Secure Electronic Records
15. Secure Electronic Signature

Chapter vi: Regulation of Certifying Authorities

The regulation of Certifying Authority (CA) is a statutory function of the Controller of Certifying Authority (CCA) and under the IT Act he has to act as administrative authority rather than quasi-judicial body. Following are the sections covered under this provision:

17. Appointment of Controller and other officers
18. Functions of Controller
Chapter 2: Introduction to Indian IT Act 2000/2008

19. Recognition of foreign Certifying Authorities
20. Controller to act as repository
21. License to issue electronic signature certificates
22. Application for license
23. Renewal of license
24. Procedure for grant or rejection of license
25. Suspension of License
26. Notice of suspension or revocation of license
27. Power to delegate
28. Power to investigate contraventions
29. Access to computers and data
30. Certifying Authority to follow certain procedures
31. Certifying Authority to ensure compliance of the Act, etc.
32. Display of license
33. Surrender of license
34. Disclosure

Chapter vii: Electronic Signature Certificates

Any person may make an application to the Certifying Authority for the issue of an Electronic Signature Certificate in such form as may be prescribed by the Central Government. Following are the sections covered under this provision:

35. Certifying Authority to issue Electronic Signature Certificate
36. Representations upon issuance of Digital Signature Certificate
37. Suspension of Digital Signature Certificate
38. Revocation of Digital Signature Certificate
39. Notice of suspension or revocation

Chapter viii: Duties of Subscribers

Subscriber is a person in whose name the Electronic Signature Certificate is issued. To become a subscriber, apply to the Local Registration Authority of a licensed Certifying Authority in a prescribed application form for getting the Digital Signature Certificate or Electronic Signature Certificate. Following are the sections covered under this provision:
40. Generating Key Pair
   40-A. Duties of subscriber of Electronic Signature Certificate
41. Acceptance of Digital Signature Certificate
42. Control of Private Key

Chapter ix: Penalties, Compensation and Adjudication

If any person without permission of the owner or any other person who is in-charge of a
computer, computer system or computer network does any of the acts defined in the
rules, then he shall be liable to pay damages by way of compensation to the person so
affected. Following are the sections covered under this provision:

43. Penalty and Compensation for damage to computer, computer system, etc.
   43A. Compensation for failure to protect data
44. Penalty for failure to furnish information, return, etc.
45. Residuary Penalty
46. Power to Adjudicate
47. Factors to be taken into account by the adjudicating officer

Chapter x: The Cyber Appellate Tribunal

The Central Government shall, by notification, establish one or more appellate tribunals
to be known as the Cyber Appellate Tribunal. The Central Government shall also
specify in the notification, the matters and places in relation to which the Cyber
Appellate Tribunal may exercise jurisdiction. Following are the sections covered under
this provision:

48. Establishment of Cyber Appellate Tribunal
49. Composition of Cyber Appellate Tribunal
50. Qualifications for appointment as Chairperson and Members of Cyber Appellate
    Tribunal
51. Term of office, conditions of service etc. of Chairperson and Members
52. Salary, allowance and other terms and conditions of service of Chairperson and
    Member
   52A Powers of superintendence, direction, etc.
   52B Distribution of Business among Benches
Chapter xi: Offences

Any person who knowingly or intentionally conceals, destroys or alters, or causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to 3 years or with fine which may extend up to Rs. 2 lakh or with both.

The ‘computer source code’ means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Following are the sections covered under this provision:

65. Tampering with Computer Source Documents
66. Computer Related Offences
   66A Punishment for sending offensive messages through communication service, etc.
   66B Punishment for dishonestly receiving stolen computer resource or communication device
66C Punishment for identity theft
66D Punishment for cheating by personation by using computer resource
66E Punishment for violation of privacy
66F Punishment for cyber terrorism

67. Punishment for publishing or transmitting obscene material in electronic form
   67A Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form
   67B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form
   67C Preservation and Retention of information by intermediaries

68. Power of Controller to give directions:
   69. Powers to issue directions for interception or monitoring or decryption of any information through any computer resource
      69A Power to issue directions for blocking for public access of any information through any computer resource
      69B Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security

70. Protected system
   70A National nodal agency
   70B Indian Computer Emergency Response Team to serve as national agency for incident response

71. Penalty for misrepresentation
72. Penalty for breach of confidentiality and privacy
   72A Punishment for Disclosure of information in breach of lawful contract

73. Penalty for publishing electronic Signature Certificate false in certain particulars
74. Publication for fraudulent purpose

75. Act to apply for offence or contraventions committed outside India
76. Confiscation

77. Compensation, penalties or confiscation not to interfere with other punishment
   77A Compounding of Offences
   77B Offences with three years’ imprisonment to be cognizable

78. Power to investigate offences
**Chapter xii: Intermediaries not to be liable in certain cases**

An intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him. However, the following conditions must be fulfilled:

1. The function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted;
   or
2. The intermediary does not -
   a. Initiate the transmission,
   b. Select the receiver of the transmission, and
   c. Select or modify the information contained in the transmission;
3. The intermediary observes due diligence while discharging his duties under this Act & observes such other guidelines as the Central Govt. may prescribe in this behalf.

**Chapter xii-a: Examiner of Electronic Evidence**

For the purposes of providing expert opinion on electronic form evidence before any court or other authority, the Central Government may specify, by notification in the Official Gazette, any department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence. ‘Electronic form evidence' means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines.

Following are the sections covered under Chapter xii and xii-a provision:

79. Exemption from liability of intermediary in certain cases

79-A. Central Government to notify Examiner of Electronic Evidence
Chapter xiii: Miscellaneous

Following are the sections covered under Chapter xiii provision:

80. Power of Police Officer and Other Officers to Enter, Search, etc.
81. Act to have Overriding effect
   81A Application of the Act to Electronic cheque and Truncated cheque
82. Chairperson, Members, Officers and Employees to be Public Servants
83. Power to Give Directions
84. Protection of Action taken in Good Faith
   84A Modes or methods for encryption
   84B Punishment for abetment of offences
   84C Punishment for attempt to commit offences
85. Offences by Companies
86. Removal of Difficulties
87. Power of Central Government to make rules
88. Constitution of Advisory Committee
89. Power of Controller to make Regulations
90. Power of State Government to make rules
91. Amendment of Act 45 of 1860
92. Amendment of Act 1 of 1872
93. Amendment of Act 18 of 1891
94. Amendment of Act 2 of 1934

IT Act 2008 (Amended)

Following are the few amendments introduced in IT (Amendment) Act, 2008 over IT Act 2000:

1. Electronic signatures introduced-
2. Corporate responsibility introduced in S. 43A
3. Critique on amended section 43 of IT Act
4. Important definitions added
5. Legal validity of electronic documents re-emphasized
6. Critique on Power of Controller under the amended Act
7. The Role of Adjudicating officers under the amended Act
8. Composition of CAT
9. New cybercrimes as offences under amended Act-
10. Section 67 C to play a significant role in cybercrime prosecution
11. Section 69- Power of the controller to intercept amended
12. Section 69B added to confer Power to collect, monitor traffic data
13. Power to block unlawful websites should be exercised with caution
14. Significance of the term “Critical Information Infrastructure"
15. Important clarifications on the Act’s application & effect
16. The combined effect of Section 77 and 77 B
17. Combined effect of Section 78 & 80
18. Liability of Intermediary amended
19. Examiner of Electronic Evidence created

Chapter Summary

- Introduction to Indian IT Act 2000/2008
- The Indian IT Act 2000 as amended by The IT (Amendment) Act, 2008 contains 13 Chapters
- ‘Electronic form evidence’ means any information of probative value that is either stored or transmitted in electronic form.

Exercises

1. Describe the main aims and objectives of the IT Act, 2000?
2. What is Electronic signature and Digital Signature?
3. What is the meaning of Cyber Appellate Tribunal?
4. How do you use the ‘Electronic form evidence’ in Central Government or a State Government office?
5. Mention the provision of IT Act under which State Government can make rules.
Chapter 3

IT Act and Provisions of Electronic Delivery of Government Services

Chapter Objectives:

In order to provide the Government Services in electronic mode, the IT Act, 2000 and 2008(amended) has provided some special provisions. These provision enables Government to notify services for electronic delivery, fix user charges and its sharing, appointment of authorized service provider/agents for delivery of services, creation of repository of digitally signed records and other matters related in electronics delivery of the services to the citizen. Many States in the country under the IT Act, 2000 and 2008(amended) have notified Electronic Service Delivery Rules. In this chapter, the specific provision of the IT Act which enables Government to provide electronic services electronically shall be discussed.

Chapter in a Nutshell:

THE ELECTRONIC DELIVERY OF SERVICES

NEED FOR THE ELECTRONIC DELIVERY OF SERVICES RULES
BENEFITS OF THE ELECTRONIC DELIVERY OF SERVICES RULES
KEY FEATURES OF OTHER STATE RULES
The Electronic Delivery of Services

The IT Act, 2000 & 2008 (amended) provides for the use of electronic records and digital signature by the Central and State Government and also empowers both Government to authorize the service providers for delivery of services to the citizen.

Keeping this in mind the DeitY, Government of India has developed a model electronic service delivery rule towards the help of State government in accelerating the delivery of public services in electronic mode. The States are customizing the rules as per their requirements for providing necessary directions to all concerned departments in the State Government for electronic delivery of public services.

![Fig 3.1: e-Governance Project for delivery services in Electronics Mode](image)

Need for the Electronic Delivery of Services Rules

The shifting from traditional manual service delivery to electronic service delivery requires understanding and compliance with the technological and other quality standards such as defined services charge, norms of service delivery and access channels etc., which very often department finds difficult to comply with and implement due to nonexistent rules, procedure as well as lack of state level coordination mechanism for necessary guidance.

In order to fulfill the above requirements for smooth delivery of government services in electronic mode, the Government of India has proposed model electronics service delivery rules in 2011 within the ambit of the IT Act, 2000. The model rules further being customized by the different States as per their need.

These rules have been proposed as per the provision of the Rules and exercise of power conferred by sub-section (1) of section 90 read with Section 6 and 6A of the Information Technology Act, 2000 & IT Act 2000 (amended). The details of the provisions are as follows:
Sec 90 - Power of State Government to make rules under IT Act:

1. The State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.
2. In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:
   a. the electronic form in which filing, issue, grant receipt or payment shall be effected under sub-section (1) of section 6;
   b. for matters specified in sub-section (2) of section 6;

**Note:** The State Govt. may customize the ESD rules as per their own requirement. It is understood that Government of Assam is also in the advanced stage of finalizing the ESD rules for the state.

Sec 6 - Use of electronic records and electronic signatures in Government and its agencies:

Use of electronic records and digital signatures in Government and its agencies:

1. Where any law provides for:
   a. the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;
   b. the issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner;
   c. the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

2. The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe:
   a. the manner and format in which such electronic records shall be filed, created or issued;
   b. the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a)
Sec 6A- Delivery of Services by Service Providers:

i) The appropriate Government may for the purpose of efficient delivery of services to the public thorough electronic means, authorise by order, any service provider to set up, maintain, upgrade, the computerised facilities and perform such other services as it may specify by notification in the official gazette.

ii) The appropriate Government may also authorise any service provider authorise under section (i) to collect, retain and appropriate such service charges as may be prescribed by the appropriate Government for the purpose of providing such services, from the person availing such services.

iii) Subject to provision of sub section ii), the appropriate Government may authorise, the service provider to collect, retain, appropriate service charges under this section notwithstanding the fact that there is no express provision under the Act, rules, regulation or notification under which the service is provided to collect, retain and appropriate e-service charges by the service provider.

iv) The appropriate Government by notification in the Official Gazette specify scale of services charges which may be charged and collected by the service provider.

Some of the important provisions of the rules are as follows:

a. Constitution of Directorate of Electronics and Information Technology under IT Department for enforcing the provisions of the rules and for establishing better coordination with all stakeholders.

b. Appointment and monitoring of the Authorized service providers and Authorized Service Agents for service delivery

c. Notification of Public services for electronic delivery by the department/s

d. Specifying user charges to be paid for the services to be delivered through authorized service agents and its sharing amongst the stake holders

e. Use of electronic signature in delivery of services and creation of State level electronic records repositories

f. Notifying signing authorities by the Departments for use of electronic signatures

g. Creation of secured software for service delivery by the departments

h. Creation of State electronic records repository of digitally signed documents of the Government

i. IT Audit of the system and software to be used for electronic service delivery by Departments
Benefits of the Electronic Delivery of Services Rules

The implementation of the rules will likely to provide much needed direction and standardized the process of service delivery but will also establish a state level mechanism where in accountability and deficiency on the part of service provider can be easily tracked for effective monitoring and corrective measures. The rules will also help the State in leveraging the private sector assistance in the delivery of Government services and collection of necessary service charge fixed by the department from the citizen.

Further, it will also give impetus to the wide scale use of electronic signature and acceptance of electronically signed documents in the day to day government transaction with the citizen, employee and business etc. which are much more secured, authenticated and having greater life span. The creation of state level electronics records of repository will help in over the counter services delivery of services, easy authentication, online verification and lifelong preservation of such documents.

Fig 3.2: Sample Structure of ESD Governance
Key Features of Other State Rules

- Chhattisgarh - To carry out e-Governance in respect of Notified Citizen Services
- Gujarat - Regulates Cyber Cafes
- Karnataka - Provides for delivery of e-Services pertaining to matters specified in Schedule I of these rules
- Kerala - Provides for e-services through departmental access points or through electronically enabled kiosks.
- MP - Regulates electronic delivery of citizen services and appointment of service provider and provides a list of services to be delivered through the Authorised Agent and the Departments
- AP - Envisages delivery of public services in electronic mode within 5 years and appoints a Director of Electronic Service Delivery for managing the front-end of the delivery

Chapter Summary

- Need of the ESD Rules
- Provision under IT Act which enables States to make Electronic Service Delivery Rules.
- Various Important provision of ESD Rules

Exercises

1. Under what provision of IT Act Electronic Service Delivery Rules is framed?
2. What are important provisions of the ESD Rules?
3. Explain benefits of the electronic delivery of services rules in India.
Chapter 4

Program and Infrastructure of Delivery of e-Services

Overview:

The National e-Governance Plan approved by the Government of India in May, 2006 envisages to make all Government services accessible to the common man in his locality, through common service delivery outlets. The second Administrative Reforms Commission has recommended a clear road map with set of milestones to be outlined by Government of India with the ultimate objective of transforming the citizen and Government interaction at all levels to the e-Governance mode by 2020. This chapter gives a fair understanding about Program and Infrastructure of Delivery of e-Services under the Government of India’s National e-Governance Plan.

Chapter in a Nutshell:

INTRODUCTION TO E-GOVERNANCE
NATIONAL E-GOVERNANCE PLAN (NEGP)
   IMPLEMENTATION STRATEGY, APPROACH AND METHODOLOGY OF NEGP
   PROJECTS IDENTIFIED UNDER NEGP
   INSTITUTIONAL FRAMEWORK
   PEOPLE INFRASTRUCTURE
   NEGP CORE INFRASTRUCTURE
ASSAM STATE WIDE AREA NETWORK (ASWAN) STRUCTURE
   STATE WIDE AREA NETWORK (SWAN)
   SWAN ARCHITECTURE
   IMPLEMENTATION MODEL
   SWAN FOR DEPARTMENT: STRATEGY
   STATE DATA CENTRE (SDC)
   ASSAM STATE DATA CENTER
SSDG - STATE SERVICE DELIVERY GATEWAY
   OBJECTIVES OF SSDG
   STATE PORTAL
   SP-SSDG PROJECT IN ASSAM
   SSDG INTEGRATION WITH MMPs
Chapter 4: Program and Infrastructure of Delivery of e-Services

**NSDG**

**COMMON SERVICES CENTRES (CSC)**
- Assam Common Services Centers (CSC) Project
- CSC Online Monitoring Tool

**CLOUD COMPUTING**
- Architectural Vision of GI Cloud
- GI Cloud Reports

**INDIA’S E-GOVERNANCE STANDARDS**

**USE OF FREE AND OPEN SOURCE SOFTWARE**
- E-Authentication or E-Pramaan
- Benefits of E-Authentication
- Overview of E-Authentication Mechanisms
- Levels of Authentication Assurance

**M-GOVERNANCE**
- Mobile Seva

**E-MAIL SYSTEM**
- E-Mail Views
- Read New Email
- Send Email
- Instructions for New E-Mail User Registration
- Limits at Mail Gateways
- Limits for Mail Clients
- E-Mail: Dos and Don’ts
National e-Governance Plan (NeGP)

The National e-Governance Plan (NeGP), in India was introduced on 18th May, 2006, by the Department of Electronics and Information Technology (DeitY) and Department of Administrative Reforms and Public Grievances (DARPG), Government of India. It comprises of core Infrastructure projects and 31 different Mission Mode Projects (MMPs). It is expected that proper implementation of the NeGP would lay the foundation and provide the impetus for long-term growth of e-Governance within the country.

Vision:

To make all Government services accessible to the common man in his locality, through common service delivery outlets and ensures efficiency, transparency and reliability of such services at affordable costs to realize the basic needs of the common man.

In order to makes this happen, the Central Government has taken initiative in creating a common core and support infrastructure consisting of:

- State Wide Area Networks, State Data Centers, Common Services Centers and State Service Delivery Gateways
- Evolving and laying down Standards and Policy Guidelines to ensure sharing of information and seamless interoperability of data and e-Governance applications.
- Identification and Implementation of Mission Mode in various Ministries with high citizen-centric interface.

Implementation Strategy, Approach and Methodology of NeGP

Implementation of e-Governance is a highly complex process requiring provisioning of hardware and software, networking, process re-engineering and change management. Based on lessons learnt from the past and the experience from successful e-Governance applications, the approach and methodology adopted for NeGP contains the following elements:

a) Ownership of Ministries: Under the NeGP, various MMPs are owned and spearheaded by the concerned line Ministries. In case there are any ongoing projects which fall in the MMP category, they would be suitably enhanced to align them with the objectives of NeGP. For major projects like Bharat Nirman, Rural Employment Guarantee Schemes, etc. the line ministries concerned are
 advised to make use of e-Governance as also automation techniques from the inception stage. States have been given the flexibility to identify a few additional state-specific projects, which are relevant for the economic development of the State.

b) **Common Support Infrastructure:** NeGP implementation involves setting up of common and support IT infrastructure such as: State Wide Area Networks (SWANs), State Data Centres (SDCs), Common Services Centres (CSCs) and Electronic Service Delivery Gateways.

c) **Facilitator role of DeitY:** DeitY is the facilitator and catalyst for the implementation of NeGP by various Ministries and State Governments and also provides technical assistance. It serves as a secretariat to the Apex Committee and assists it in managing the program. In addition, DEITY is also implementing pilot/infrastructure/technical/special projects and support components. DARPG’s responsibility is towards Government Process Re-engineering and Change Management, which are desired to be realised across all government departments. Planning Commission and Ministry of Finance allocate funds for NeGP through Plan and Non-plan budgetary provisions and lay down appropriate procedures in this regard.

d) **Integrative Elements:** Adoption of unique identification codes for citizens, businesses and property is to be promoted to facilitate integration and avoid ambiguity.

e) **Programme Approach at the National and State levels:** For implementation of the NeGP, various Union Ministries/Departments and State Governments are involved. Considering the multiplicity of agencies involved and the need for overall aggregation and integration at the national level, NeGP is being implemented as a programme, with well-defined roles and responsibilities of each agency involved. For facilitating this, appropriate programme management structures have also been put in place.

f) **Governance:** Suitable arrangements for monitoring and coordinating the implementation of NeGP under the direction of the competent authorities have also been substantially put in place. The programme also involves evolving/laying down standards and policy guidelines, providing technical support, undertaking capacity building, R&D, etc. Department of Electronic and Information Technology (DEITY) is required to adequately strengthen itself and various institutions like NIC, STQC, CDAC, NISG, etc. to play these roles effectively.

g) **Public-Private Partnerships (PPP):** PPP model is to be adopted wherever feasible to enlarge the resource pool without compromising on the security aspects.

h) **Centralised Initiative, Decentralised Implementation:** E-Governance is be-
ing promoted through a centralised initiative to the extent necessary to ensure citizen-centric orientation, to realise the objective of inter-operability of various e-Governance applications and to ensure optimal utilisation of ICT infrastructure and resources while allowing for a decentralised implementation model. It also aims at identifying successful projects and replicating them with required customisation wherever needed.

Fig. 4.2: Institutional Framework of Government of India for NeGP Implementation

In order to promote e-Governance in a universal manner, various policy initiatives and projects have been undertaken to develop core and support infrastructure. The major core infrastructure components are:

- State Data Centres (SDCs)
- State Wide Area Networks (S.W.A.N)
- Common Services Centres (CSCs)
- Middleware gateways i.e. National e-Governance Service Delivery Gateway (NSDG)
- State e-Governance Service Delivery Gateway (SSDG)
- Mobile e-Governance Service Delivery Gateway (MSDG)

The important support components include Core policies and guidelines on Security, HR, Citizen Engagement, Social Media as well as Standards related to Metadata, Interoperability, Enterprise Architecture, Information Security etc. New initiatives include a framework for authentication, viz. e-Pramaan and G-I cloud, an initiative which will ensure benefits of cloud computing for e-Governance projects.

Mission Mode Projects (MMPs) are individual projects within the National e-Governance Plan (NeGP) that focus on one aspect of electronic governance, such as banking, land records or commercial taxes etc. Within NeGP, "mission mode" implies that projects have clearly defined objectives, scopes, and implementation timelines and milestones, as well as measurable outcomes and service levels. NeGP comprises different mission mode projects (MMPs), which are further classified as state, central or integrated projects.
Projects Identified Under NeGP

a) Mission Mode Projects (MMPs)

Following are the mission mode projects under NeGP, Government of India’s Mission Mode Projects (MMPs)

Mission Mode Project

<table>
<thead>
<tr>
<th>CENTRAL - 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking</td>
</tr>
<tr>
<td>Insurance</td>
</tr>
<tr>
<td>income Tax</td>
</tr>
<tr>
<td>Central Excise</td>
</tr>
<tr>
<td>MCA 21</td>
</tr>
<tr>
<td>Pensions</td>
</tr>
<tr>
<td>Passport</td>
</tr>
<tr>
<td>e-office (Pilot)</td>
</tr>
<tr>
<td>National ID / UID</td>
</tr>
<tr>
<td>Immigration / Visa</td>
</tr>
<tr>
<td>Posts</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STATE - 14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Land Rec / NLRMP</td>
</tr>
<tr>
<td>Transport</td>
</tr>
<tr>
<td>e-District</td>
</tr>
<tr>
<td>Commercial Taxes</td>
</tr>
<tr>
<td>Treasuries</td>
</tr>
<tr>
<td>Municipalities</td>
</tr>
<tr>
<td>Police - CCTNS</td>
</tr>
<tr>
<td>Agriculture</td>
</tr>
<tr>
<td>Panchayats</td>
</tr>
<tr>
<td>Employment Exchange</td>
</tr>
<tr>
<td>Health</td>
</tr>
<tr>
<td>Education</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>INTEGRATED - 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>India Portal</td>
</tr>
<tr>
<td>NSOO</td>
</tr>
<tr>
<td>CSC</td>
</tr>
<tr>
<td>e-Courts</td>
</tr>
<tr>
<td>EOI</td>
</tr>
<tr>
<td>e-Biz</td>
</tr>
<tr>
<td>e-Procurement</td>
</tr>
</tbody>
</table>

Total No. of Service Categories planned: 274 (84 Control, 140 State, 51 Integrated)
Institutional Framework for Implementation

- Capacity Building Scheme for States
  - To create capacities in States for project management & implementation
  - By tapping government & private sector talent
  - To train & sensitize employees
  - To undertake change management
  - To orient project implementation towards service delivery
**NeGP Core Infrastructure**

![Diagram of e-Governance core infrastructure](image)

**State Wide Area Network (SWAN)**

The Government has approved the Scheme for establishing State Wide Area Networks (SWANs) across the country. Under this Scheme, technical and financial assistance are being provided to the States/UTs for establishing SWANs to connect all State/UT Headquarters up to the Block level via District/ sub - Divisional Headquarters, in a vertical hierarchical structure with a minimum bandwidth capacity of 2 Mbps per link. Each of the State / UT can enhance the bandwidth up to 34 Mbps between SHQ and DHQ and upto 8 Mbps between DHQ and BHQ depending upon the utilization. Steps have been initiated to integrate all SWANs using the National Knowledge Network (NKN).

SWAN is envisaged as the converged backbone network for data, voice and video communications throughout a State/UT with the following salient features:

- One PoP at each State / District / Block Headquarter
- Each PoP has Configurable Aggregation Equipment to enable vertical & horizontal connectivity
- Gateway to NICNET (National Backbone) for Inter-State connectivity
- State/ NIC would receive discounted price for BSNL BW cost (MoU signed)
- The intranet for the State Government.
- It will connect all offices of the State Govt. with each other providing data, voice & video services as required through the state.
Implementation Model

There are two Options for SWAN implementation as detailed below:

**Option I – Public Private Partnership (PPP) Model** State identifies a suitable PPP model (BOO, BOOT etc.) and selects an appropriate agency through a suitable competitive process for outsourcing the establishment, operation and maintenance of the Network.

**Option II – NIC Model** State designates NIC (National Informatics Centre) as the prime implementation agency for SWAN for establishment, operation and maintenance of the Network.
Assam State Wide Area Network (ASWAN) Structure

The project State Wide Area Network for the State of Assam is implemented by the State designated SWAN Implementing Agency i.e., M/s. AMTRON Ltd., Guwahati in PPP mode. Under the state of Assam SWAN, 304 nos. of PoP have been planned across the state.

Some of the important features of ASWAN are:-

- Backbone network for data, Voice & Video communications.
- 3tire Architecture with 304nos POP
- Bandwidth scalable upto 155 mbps vertically
- Multiple bandwidth providers (BSNL, Railtel, Powergrid)
- Radio/wireless in difficult/remote areas
- Integrated voice over IP phone(VOIP) and video conference
- Integrated e-mail server
- IPv6 complaint
- 304 nos POP commissioned across state. State HQ -1,Dist HQ- 27 POPs, balance setup across block and circle offices.

SWAN for Department: Strategy

- IT Dept. responsible for creation of vertical network of ASWAN
- Depts. to connect their offices from POPs at SHQ/DHQ/BHQ
- Connectivity is not free- needs budgetary provision by the dept.
- Fixed cost of physical media (wire/wireless/radio etc.)
- Opex (bandwidth/maintenance/replacement if any)
- Design the network in consultation with AMTRON
- AMTRON will soon standardize the solution for Hz connectivity along with cost for other deptt.
State Data Centre (SDC)

State Data Centre (SDC) has been identified as one of the important element of the core infrastructure for supporting e-Governance initiatives of National e-Governance Plan (NeGP).

Under NeGP, it is proposed to create State Data Centers for the States to consolidate services, applications and infrastructure to provide efficient electronic delivery of G2G, G2C and G2B services. These services can be rendered by the States through common delivery platform seamlessly supported by core Connectivity Infrastructure such as State Wide Area Network (SWAN) and Common Service Centre (CSC) connectivity extended up to village level. State Data Centre would provide many functionalities and some of the key functionalities are Central Repository of the State, Secure Data Storage, Online Delivery of Services, Citizen Information/Services Portal, State Intranet Portal, Disaster Recovery, Remote Management and Service Integration etc. SDCs would also provide better operation & management control and minimize overall cost of Data Management, IT Resource Management, Deployment and other costs.

Department of Information Technology (DIT) has formulated the Guidelines to provide Technical and Financial assistance to the States for setting up State Data Centre.

Fig 4.8: State Data Centre Reference Architecture
Assam State Data Center

Features of Assam State Data Center

- State repository of electronic database
- Shared, reliable and secured infrastructure service center for hosting and managing the e-Government applications of departments.
- Largest Data center of NE region with 22,000 Sq. ft. build up area and with 75 TB+ capacity
- Only cloud enabled SDC of the eastern region
- Tire 3 SDC with highly scalable model
- Disaster recovery mechanism for business continuity
- All certification of International standards
- 24X7 availability with all security measures
- Expected to be operational by March 2015

Data center- Services for the departments:

1. **Co-location of the server infrastructure**
   a) Departments to bring existing servers
   b) Department to buy new servers as per requirement
   c) Rack space would be provided
   d) Other data Center services would be available
   e) Depts. to deploy its own manpower for maintenance

2. **Hosting of services for software application**
   a) Data center servers would be made available
   b) DCO shall support in hosting & maintenance of applications
   c) Depts. do not require to deploy manpower

3. **Advanced data center services**
   a) Data center servers would be made available
   b) Data base tuning /application enhancement
   c) Facility for data base migration by DCO
   d) Database/application administration
   e) Depts. do not require to deploy manpower

4. **Disaster/ Data Base recovery solution**
   a) State Data Center would be integrated with a DR site
   b) Ensure business continuity
5. Data Center-Departments Strategy-1 & 2

Does not require to built-up additional civil & electrical infrastructure

1. Capex
   i) Cost provisioning of the Servers/storage etc. in the DPR
   ii) Warranty and support must be factor for long term (say 5 years)

2. Opex
   i) Security Certification of application to be hosted in SDC at periodic level or for new application
   ii) No application would be allowed to be hosted without security testing
   iii) Data base migration cost from one platform to another

Optimize the Sever and data base requirements/ sizing at design stage in consultation with IT Deptt/ AMTRON

SSDG & State Portal (State Service Delivery Gateway and State Portal)

The State e -Governance Service Delivery Gateway (SSDG), a core component in e-Governance infrastructure under the NeGP, can simplify this task by acting as a standards-based messaging switch and providing seamless interoperability and exchange of data across. This project aims to enhance the services provided to the citizens through Common Service Centers (CSCs) by carrying out the Implementation of the State Portal, State Service Delivery Gateway (SSDG) & Electronic Form application. It is envisaged that the common infrastructure (SWAN, SDC & CSC) would be leveraged immediately by developing applications and infrastructure required for deployment of State Portals (SP) and State Service Delivery Gateway (SSDG) across the States/UTs. This will enable citizens to download forms and submit their applications electronically through a common gateway. This important initiative facilitating electronic Service Delivery will provide significant benefits to the citizens especially in the form of a single gateway to citizen for service delivery.
Objectives of SSDG

Easy, anywhere and anytime access to Government Services via e-form:

Enables integrated service delivery by:

i. Online/Offline e-filing of application through e-forms through different channel via State Portals

ii. Intelligent routing of forms to the destination field office by SSDG

- Enable assured electronic delivery, acknowledgement and status tracking of application
- Facilitate online payments
- Integration with NSDG
- MIS reporting at the State level
- E-transaction recorded at National level (e-taal)
State Portal (SP):

The State Portal has been envisaged to cater to providing information, and delivering online services (G2C, G2G & G2B) via integrated web applications. The main features are as follows:

- **Single point of access**: Thus the Portal shall act as an Integrated Services Delivery Channel for all departments in the State

- **Citizen Relationship**: Shall be the virtual face, where an end-user can access information or interact with the government, any time from any place from the Internet / CSCs/other channels

- **Cater to Government’s Long Term Strategy**: Most importantly the portal is the vehicle to the Government’s long term strategy of paperless, improved governance including transparency and accountability.

SP-SSDG Project in Assam

The Government of Assam has notified www.assam.gov.in as the State Portal of Assam and the project has already been commissioned. The portal apart from having SSDG as a messing middle ware will also facilitate SMS and payment gateway. The Portal would be the hub for all interaction between service seekers (citizens, businesses) and service providers (Government Departments). Acting as a nerve center the portal would handle transactions across the entire network and will be a single point of access. This infrastructure would also help inter-departmental working in a co-ordinated and synchronized manner. As a central message processing mechanism it would also help in tracking Government transactions, which would be further linked to the National Service Delivery Gateway to ensure a single window of service for all government services/interaction across the country.

In Assam, 'Assam Electronic Development Corporation' Ltd (AMTRON) is the State Nodal Agency for implementation of the Project.

e-Forms Application

- It is envisaged to facilitate the submission of electronic forms for G2C, G2G & G2B services.

- Availability of online and down-loadable forms for easy access through /from different delivery channels.

- Acknowledgement on the receipt of the same with unique id for tracking the status

- E-forms Application integration with the departments back end workflow
SSDG Integration with MMPs

The following three scenarios will explain e-Forms integration with the MMPs.

- Scenario 1: State Deptt. with Non-Automated backend IT System
- Scenario 2: State Deptt. with Automated backend IT System
- Scenario 3: State Deptt. with Partially Automated backend IT System

Scenario 1

![State Dept. with None-Automated back end IT System](image1)

Fig 4.10: State Dept. with None-Automated back end IT System

- Dept. Back-end is not automated with workflow
- So E-form cannot be integrated with Dept. Application work-flow.
- Centralized application (SSDG) with minimum work-flow can be implemented
- SSDG will intelligently route to the centralized application only
- Deptt. users will login into this application & process services manually

Acknowledgement is received from this centralized application & routed to the State Portal for delivery to the citizen.

Scenario 2: State Department with Automated back-end System:

![State Dept. with Automated Backed IT System](image2)

Fig 4.12: State Dept. with Automated Backed IT System
Chapter 4: Program and Infrastructure of Delivery of e-Services

- Dept. Back-end is automated with workflow
- So E-form is to be integrated with Dept. Application workflow.
- SSDG will intelligently route the Services for G2C and G2G
- Department users will login into Dept. application and process the various services
- Acknowledgement is received from SSDG/Deptt application and routed to the State Portal for delivery to the citizen.

Scenario-3: State Department with Partially Automated Backend IT system

![State Dept. with Partially Automated Backend IT System](image)

- Dept. Back-end is partially automated with few services.
- So E-form will be integrated partially with e-ready service of dept. application.
- Partially e-ready services can be hosted on SSDG
- Request obtained will intelligently route the services to department.
- Department shall manually process the services and sent it back to SP
- Acknowledgement is received from SSDG/Dept. Application.

NSDG

One of the goals of the Government to meet this vision is the need to cooperate, collaborate and integrate information across different departments in the Centre, States and Local Government. Government systems characterized by islands of legacy systems using heterogeneous platforms and technologies and spread across diverse geographical locations, in varying state of automation, make this task very challenging. The National e-Governance Service Delivery Gateway (NSDG), a MMP under the NeGP, can simplify this task by acting as a standards-based messaging switch and providing seamless interoperability and exchange of data across.
The objectives of the NSDG are:

- To act as a core infrastructure for achieving standards-based interoperability between various e-Government applications implemented at various levels and geographically dispersed locations.
- To evolve Gateway messaging standards and build a government owned Central Gateway based on these standards.
- Act as a catalyst in enabling the building of Standards based e-Governance applications with Gateway as the middleware to ensure interoperability.
- Enable integration across Centre, State or Local Governments there by enabling Integrated Service Delivery and a Service Oriented Architecture (SOA) leading to joined up government.
- Help protect the legacy investments in software and hardware by easily integrating them with other technology platforms and software implementations.
- De-link the back-end departments/Service Providers (SP) from the front-end Service Access Providers thereby ensuring separation of concerns of service access from the service implementation i.e. separates the Portal, CSC, Kiosks etc from the government services which reside in the backend departments.
- Encouraging competition at the front-end by allowing independent service access providers to provide services with varying levels of complexity, cost and service quality levels.
- Shared services can be added on to the core services as and when required, as special common services of the Gateway without affecting the core functionality of the Gateway, thereby providing flexibility and modularity.
- Reduce the cost of e-Governance Projects by rationalizing, distributing and optimizing the services framework.
- Use PKI infrastructure for secure transactions. Provision exists for encryption of department payload to ensure confidentiality of department data. The gateway provides digital signature and certificates to all stakeholders interacting with the gateway for identification, authentication and authorization. Transaction and audit logs help track government data.
- Enable transaction logging and time stamping for tracking of transactions and centralized control.

Help the Departments backend workflow evolve gradually as the Gateway acts as a middleware de-linking the backend from the front end. This means that even the Departments which do not have the complete automation or work flow at the back can still deliver e-Service to the citizens in a limited manner through
the Gateway. To cite as an example, a server may be put up at the department for message exchange with Gateway in absence of readily available infrastructure at the department.

Common Services Centres (CSC)

The CSC is a strategic cornerstone of the National e-Governance Plan (NeGP), approved by the Government in May 2006, as part of its commitment in the National Common Minimum Programme to introduce e-governance on a massive scale. The CSCs would provide high quality and cost-effective video, voice and data content and services, in the areas of e-governance, education, health, telemedicine, entertainment as well as other private services. A highlight of the CSCs is that it will offer web-enabled e-governance services in rural areas, including application forms, certificates, and utility payments such as electricity, telephone and water bills.

Background of the Scheme:

• The Common Services Centres (CSCs) Scheme was approved by the Government of India in September 2006 to setup one lakh ICT enabled front-end service delivery outlets equitably spread across rural India. CSCs were envisaged as internet enabled centres that would allow citizens to access government, private and social services at their doorstep.

• This unique Scheme leverages information and communication technologies to drive change in rural India through entrepreneurship and market mechanisms. The inability to use or access ICTs raises the barriers towards employment, economic growth and social development. These barriers are even more accentuated for rural citizens due to differential access to education, communication assets and opportunities for learning.
Accordingly, the CSC Scheme has been designed not merely to build infrastructure, but to create a digital highway that would empower the digitally excluded; changing the way rural citizens learn, communicate, manage their livelihoods and access health, financial and government services.

- The CSC scheme has been designed and implemented under the National e-Governance plan (NeGP) using a three tier Public Private Partnerships (PPP) based implementation strategy. The CSCs are operationalised by implementation agencies called as Service Centre Agencies (SCA) appointed for each division by State Designated Agencies (SDA). Village Level Entrepreneurs (VLEs) are appointed by the SCAs to operate CSCs at pre-defined locations within a cluster of villages.

- The CSCs are operationalised on 1:6 ratio with one CSC servicing about 6 villages. This ensures equitable spread of one lakh CSCs across 6,00,000 villages of the country. Further, about 10,000 urban CSCs were also expected to be operationalised.

- A typical CSC comprises of PC(s), printer(s), scanner(s), UPS, digital/web camera and broadband connectivity. Additional equipment in the form of projection systems, and biometric devices, etc. has been included where relevant and sustainable.

- The Scheme was designed to provide viability gap funding to the private partners. The Scheme assumed that the private sector- SCA & VLE- would pay for the capital expenses as well as operational costs associated with setting up and operationalising CSCs. These costs were to be recovered through income generated from service charges levied on the online delivery of various G2C and B2C services.

- The Scheme was expected to be implemented and operated over a period of 5 years, with viability gap funding payable for only rural CSCs as per the 1:6 ratio for a period of 48 months. It was expected that at the end of the 5 years, the CSCs would become self-sustaining. The States were also given the option of increasing the number of CSCs planned to be operationalised for which no additional revenue support was to be provided by GoI. Further, States could roll out urban CSCs, without revenue support from GoI, to cross subsidize rural CSCs. Further, it was anticipated that SCAs would adopt a franchisee model to roll out CSCs by signing agreements with VLEs. It was envisaged that the State would have a direct relationship only with the SCA and not the VLE.

- The onus of driving the implementation of the Scheme lay with the SCAs. While the CSCs were the operational partners and States and DeitY provided the financial support and monitored the Scheme implementation, the SCA’s business model determined how the Scheme would be implemented in the division. Further, the SCA’s ability to enable services through CSCs determined the sustainability of CSCs.
Arunodoy Common Services Centers (CSC) Project:

Under the scheme State plans to set up around 4375 nos. of CSCs covering around 26247 census villages (census 2001), @ 1: 6 ratio of villages. The project has been implemented in the PPP mode for which 27 districts divided into 3 zones and each zone comprises of 9 districts. In order to set up the CSCs, State selected two PPP partners namely M/s SREI Infrastructure Finance Limited and M/s Zoom Developers Limited. While M/s SREI Infrastructure Finance Limited was assigned to set up 2833 nos. of CSC in 18 district and M/s Zoom Developers Limited with 1542 nos. of CSC in 9 districts. The project execution started in 2008 and necessary agreement was signed with the PPP partners known as SCA.

SCAs are given the following primary responsibility:

a) Selection of the VLE and imparting necessary training to them

b) Help and support VLE in setting up the CSC with necessary ICT infrastructure and connectivity

c) Develop own portal for hosting necessary B2C services and tie-up with various other B2C service to CSC

d) Coordination with Government for enabling G2C services through CSC.

The brand name of Assam CSC has been coined as Arunodoy Kendra

Present Services in CSCs in Assam

The Government of Assam vide its Gazette notification in 4th August, 2009 notified 16 G2C services to be delivered through the CSCs and presently some of these services are being delivered under e-district pilot project in the districts of Goalpara and Sonitpur. These G2C services are such as:

- Permanent Resident Certificates
- Senior Citizen Certificate
- Income Certificate
- Non Creamy Layer Certificate
Chapter 4: Program and Infrastructure of Delivery of e-Services

- Next of kin Certificate
- Permission for Delayed Birth Certificate
- Permission for Delayed Death Certificate
- Certified Copy of Electoral Roll

**Business to Citizen Services**

These CSCs are also offering various relevant business to citizen services to the rural masses in cost effective way for which they have to earlier travel long distance to reach towns etc. losing their precious time, energy and money. From last year onwards CSCs are providing banking services of various nationalized banks to the rural citizen and will soon emerged as important channel of Financial inclusion in the State.

- Internet surfing
- Banking
- Education
- Recharge
- DTP
- Photography
- Scanning etc.

*Fig. 4.15: IT enabled kiosk*
Monitoring of CSC:
The four key applications developed and currently implemented which form part of the CSC monitoring solution include:

- **CSC Online Monitoring Solution**: Post CSCs are commissioned; the online monitoring tool helps in registration of CSC IT terminals and tracks uptime of IT terminals. Each CSC PC is required to install and register online monitoring tool. The online registration process serves a proof of availability of CSC IT terminals as validated by their unique machine ID (Mac ID) and internet availability for delivering digital services.

- **CSC Online Dashboard**: This tool provides executive MIS on registration and uptime status of CSCs on Pan India basis and tracks the performance of CSCs, SCAs and States based on uptime logs generated and disseminated by the online monitoring tool. [http://www.csclive.in/dashboard](http://www.csclive.in/dashboard).

- **CSC Connect**: CSC Connect is a facility available to various Service Access Provider (SAP) Portals to allow CSCs to login into their portals using their unique CSC ID / password combination defined under CSC Online Monitoring System. This facility would save CSC the trouble of registering their profiles and remembering their IDs and password with multiple SAPs. The CSC Connect mechanism would make it possible for CSCs using their unique CSC ID / Password to gain access to the SAP Portal and will also help DIT to measure the usage of services of various SAP sites at various CSCs. [http://www.csclive.in/cscconnect](http://www.csclive.in/cscconnect).

The solution currently serves the following purpose:

- Provides unique identification of a CSC based on their geography
- Maintains a centralized database of CSCs, VLE with their addresses, email and contact details.
- Enables online registration status of CSCs • Reckons uptime performance of CSCs which have been registered online on a daily basis.
- Maintains uptime Performance of a CSC, SCA and States based on CSC performance in their respective territories
- Provides role based access to all the stakeholders based on their privilege geographic usage
- Provides single waterfall view of CSCs from Pan India-State- District-Block to the ultimate CSC
- Enables recording of BSNL connectivity status at each of the CSCs as BSNL is the primary connectivity provider.
Chapter 4: Program and Infrastructure of Delivery of e-Services

Cloud Computing

What is Cloud Computing and its types?

In order to utilise and harness the benefits of Cloud Computing, Government of India has embarked upon a very ambitious and important initiative – “GI Cloud” which has been coined as “MeghRaj”. The focus of this initiative is to evolve a Strategy and implement various components including governance mechanism to ensure proliferation of Cloud in government. Formulation of the Cloud Policy is one of the primary steps that will facilitate large scale adoption of cloud by government.

The objectives of GI Cloud are as follows:

- Optimum utilisation of infrastructure
- Speeding up the development and deployment of eGov applications
- Easy replication of successful applications across States to avoid duplication of effort and cost in development of similar applications.
- Availability of certified applications following common standards at one place

Architectural vision of GI Cloud

The architectural vision of GI Cloud focuses on a set of discrete cloud computing environments spread across multiple locations, built on existing or new (augmented) infrastructure, following a set of common protocols, guidelines and standards issued by the Government of India. The GI Cloud services will be published through a single GI Cloud Services Directory.

The GI Cloud is envisaged to consist of multiple National and State Clouds.

These cloud computing environments will utilise the existing network infrastructure such as the SWANs, NKN, NOFN integration hubs as well as the internet. The figure above depicts an overview of the GI Cloud consisting of cloud computing environments at the national and state levels termed as ‘National Clouds’ and ‘State Clouds’ respectively. While one of the National Clouds will be built utilizing the infrastructure available under the National Data Centre(s), other National Clouds may also be established. These may be new or established by augmentation of the existing data centres available at state level. Based on demand assessment and taking into account security related considerations, government may also engage the services of private cloud providers. The willing state clouds built on state data centres can also associate themselves with the GI Cloud and publish their services in the GI Cloud Services Directory.

Services provided by National Clouds would include infrastructure (compute, storage and network), platform, backup and recovery, infrastructure scaling of the State Clouds,
application development, migration and hosting etc. Over a period of time, other clouds at the national level could also provide remote infrastructure management for the State Clouds.

The vision is also focused on national and state level shared, reusable applications and services that will allow any government department or agency to accelerate its e-Governance progress by using applications which other agencies or departments have already developed and made available in the government cloud environment. The National Cloud and each of the other clouds at the national level are envisaged to host an ‘eGov AppStore’ that will act as a common platform to host and run applications at National Clouds which are easily customisable and configurable for reuse by various government agencies/departments at Centre and States without investing effort in development of such applications.

**India’s e-Governance Standards**

The National e-Governance Plan was launched by the Government of India (GoI) with the intent to support the growth of e-Governance within the country. Having realized the needs of common man, it was felt that the e-Governance systems need to interoperate and for seamless sharing of data and service among the systems, standards need to be in place.

To ensure Interoperability among e-Governance applications, Government of India has setup an Institutional mechanism for formulation of Standards through collaborative efforts of stakeholders like:

- Department of Electronics and Information Technology (DeitY)
- National Informatics Centre (NIC)
- Standardization Testing and Quality Certification (STQC), and other Government departments.

E-Gov Standards may ensure and help in designing a system which can share and seamlessly enhance interoperability of the data, efficiently and effectively across e-Governance applications and their stakeholders.

The e-Governance Standards have been divided into categories like

- Policy/ Frameworks, Standards, Guidelines/ Best Practices.
- Various Expert Committees have been setup in priority areas, like Metadata and Data Standards (MDDS), Biometrics, Localisation, Security, Mobile Governance, Interoperability Framework for e-Governance in India (IFEG), Digital Signature, etc.
Objectives of e-Governance Standards

- To ensure sharing of information and seamless interoperability across e-governance applications.
- Institutional mechanism for collaborative process of standard formulation set up by DietY.
- Standards published: [http://egovstandards.gov.in](http://egovstandards.gov.in)
- Policy on open standards – Nov 2010
- Biometric standard for face image, fingerprint image and Minutiae- Nov 2010 and Iris image Standard March 2010
- Localization and language technology standards: Character encoding standard and front standard Nov:2010
- Metadata and data standards for person and land identification Dec 2010 and revised – 2011
- Technical standards under the interoperability framework for e-governance (IFEG) in India- June 2012
- Guidelines on e-governance security assurance framework (e-SAFE)
- Guidelines for Govt website Jan 2009
- Guidelines for usage of digital signature in e-governance application – Dec-2010
- Quality assurance framework and conformity assessment requirement, June 2010
- Guidelines for compliance to quality requirements of e-Procurement systems, March 2011
- Standard under progress: Interoperability framework for e-governance in India, digital preservation, Metadata and data standards for domains, mobile standards, localization guidelines for developers

Use of Free and Open Source Software

Free and Open-source software (FOSS) is revolutionizing business, transforming governments and enabling digital education across the planet. Open-source is built on the principle that the source code of a program should be readily accessible, so that users have the right to maintain, adapt and improve the software they use in any way they see fit. Linux, Firefox and Wikipedia are just three of its success stories, which are too many in number to count. Open source software is freely licensed to use, copy, study, and change the software in any way, and the source code is openly shared so that people are encouraged to voluntarily improve the design of the software whereas
in case proprietary software one can use when one has the valid license to use and has no right to customize and modify the source code.

The benefits of using FOSS can include decreasing software costs, increasing security and stability (especially in regard to malware), protecting privacy, and giving users more control over their own hardware. Free, open-source operating systems such as Linux and descendents of BSD are widely utilized today, powering millions of servers, desktops, smartphones (e.g. Android), and other devices.

Further, there are other advantages like increasing interoperability, developing local capacity/industry, reducing costs, achieving vendor independence, enabling localization, reducing piracy/copyright infringements and increasing the growth of knowledge-based society etc.

India’s strength in Information Technology can be utilized to develop products using FOSS which will help in bridging the digital divide with significant cost savings and facilitate the creation of a knowledge society. Indian industry/SMEs can benefit from the liberal licensing norms of FOSS which enables software to be freely modified and distributed.

Some important features of the word “Open source” has been said to have attributed the following features:

1. Free Redistribution. The license shall not restrict any party from selling or giving away the software as a component of an aggregate software distribution containing programs from several different sources. The license shall not require a royalty or other fee for such sale.
2. Source Code. The program must include source code, and must allow
distribution in source code as well as compiled form. Where some form of a
product is not distributed with source code, there must be a well-publicized
means of obtaining the source code for no more than a reasonable reproduction
cost preferably, downloading via the Internet without charge. The source code
must be the preferred form in which a programmer would modify the program.
Deliberately obfuscated source code is not allowed. Intermediate forms such as
the output of a pre-processor or translator are not allowed.

3. Derived Works. The license must allow modifications and derived works, and
must allow them to be distributed under the same terms as the license of the
original software.

4. Integrity of the Author's Source Code. The license may restrict source-code from
being distributed in modified form only if the license allows the distribution of
"patch files" with the source code for the purpose of modifying the program at
build time. The license must explicitly permit distribution of software built from
modified source code. The license may require derived works to carry a different
name or version number from the original software.

5. No Discrimination against Persons or Groups. The license must not discriminate
against any person or group of persons.

6. No Discrimination against Fields of Endeavour. The license must not restrict
anyone from making use of the program in a specific field of endeavour. For
example, it may not restrict the program from being used in a business, or from
being used for genetic research.

7. Distribution of License: The rights attached to the program must apply to all to
whom the program is redistributed without the need for execution of an
additional license by those parties.

8. License must not be specific to a Product. The rights attached to the program
must not depend on the program's being part of a particular software distribution.
If the program is extracted from that distribution and used or distributed within
the terms of the program's license, all parties to whom the program is
redistributed should have the same rights as those that are granted in
conjunction with the original software distribution.

9. License must not restrict other Software. The license must not place restrictions
on other software that is distributed along with the licensed software. For
example, the license must not insist that all other programs distributed on the
same medium must be open-source software.

10. License must be technology-neutral. No provision of the license may be
predicated on any individual technology or style of interface.

Open Standard:

An open standard can mean that a standard is open to anyone to use, even though it
has restrictive licensing or requires a fee. The word “Open standard” has been said to
have attributed the following features:
• Freely and publicly available – They are available free of charge and unencumbered by patents and other intellectual property.
• Non-discriminatory – They are available to anyone, any organization, anytime, anywhere with no restrictions.
• No license fees - There are no charges for their use.
• Vendor neutral - They are vendor neutral in terms of their content and Implementation concept and do not favour any vendor over another.
• Data neutral – The standards are independent of any data storage model or format.
• Agreed to by a formal, member based consensus process – The standards are defined, documented, and approved by a formal, member driven consensus process. The consensus group remains in charge of changes and no single entity controls the standards.
• The key aspect of Open Standards is that they are freely available for anyone to access and implement at any time. Software developers and development Organizations, whether create commercial or open source software, decide if they want to implement specific standards. It's important to realize that software packages, whether open source or proprietary, can interoperate if they all implement the same standard.

E-Authentication or e-Pramaan

Electronic Authentication (or “e-Authentication”) is the process of electronic verification of the identity of an entity. The entity may be a person using a computer/mobile, a computer/mobile itself or a computer/mobile program. Authentication is a way to ensure that the user who attempts to perform functions in a system is in fact the user who is authorized to do so. e- Authentication provides a simple, convenient and secure way for the users to access government services via internet/mobile as well as for the government departments and agencies to assess the authenticity of the users.

An authenticated identity is linked to the online services delivered by government departments and agencies through the process of “Authorization”. Authorization deals with the permissions or privileges granted to a user to access particular services provided by an application.

Benefits of e-Authentication

Electronic authentication helps to build confidence and trust in online transactions and encourages the use of the electronic environment as a channel for service delivery. In online transactions, data is communicated electronically through internet and mobile applications. With the increased prevalence of online transactions, there is a need to set up suitable e- authentication processes based on an assessment of the risks associated with these transactions.
Overview of e-Authentication Mechanisms

Electronic authentication is accomplished based on the following factors:

- Knowledge - something the user knows (e.g. user name, password, PIN, secret questions and answers, etc.);
- Possession - something the user has (e.g. digital signature, smart card, etc.);
- Be - something the user is (e.g. biometric fingerprint, iris pattern, etc.); or
- A combination of the above.

Utilising one or more of these factors, there may be three kinds of authentication mechanisms:

- Single Factor Authentication: An authentication mechanism that utilizes only one of the various factors (e.g., a user using username and password for accessing an application).
- Two Factor Authentication: An authentication mechanism where a combination of two factors is used (e.g., a user using username and password as first factor and One Time Password (OTP) as the second factor).
- Multi-factor Authentication: An authentication mechanism where two or more factors are used with one of the factors necessarily being the "Third Factor – ‘Be’" which is something the user is (e.g., a user providing her Aadhaar number (first factor – “Knowledge”) and her biometrics (third factor – “Be”) to authenticate herself).

Associated level of risk shall determine the appropriate authentication mechanism to be adopted. The systems, applications and information with high-level of associated risk require a stronger authentication mechanism that confirms the user's digital identity.

Authorisation of authenticated identities to access applications, services and information is accomplished based on various assigned roles. The process of authorisation assumes that the identity has been successfully authenticated. However, the authorisation process needs to verify that the sensitivity level of the e-authentication mechanism fulfills the minimum requirements of the application. If the minimum requirements are not met, a higher level of e-authentication is requested. Then, permissions assigned to the identity are verified before permitting or refusing access to the service.

Levels of Authentication Assurance

The framework provides various levels of authentication based on the sensitivity requirement of an e-Governance service.

- Level 0: No Authentication required for publicly available information.
• Level 1: User Id and Password based authentication. This is meant for basic public services with low sensitivity service.

• Level 2: Two factor authentication (User Id and Password AND OTP). Meant for personally identifiable information and services with moderate levels of security.

• Level 3: User Id and password PLUS Digital Certificate (soft/hard). Meant for services which requires high security and any or all of PAIN properties.

• Level 4: User Id and password PLUS Biometric based authentication. Meant for services requiring the highest levels of security.

The level 4 of Authentication in e-Pramaan supports UIDAI biometric authentication in which Aadhaar holders can get authenticated by giving their fingerprint which will be verified in the background through Aadhaar Authentication Server. The services of e-Pramaan will be provided through NSDG, SSDG. Central government department or state government department services registered with various service delivery gateways will call e-Pramaan services for authentication before the actual service is invoked.

Under the National e-Governance Plan (NeGP), National and State e-Governance Service Delivery Gateways (NSDG/SSDG) have been created to ensure interoperability among autonomous and heterogeneous entities of the government at both central and state levels. NSDG and SSDG infrastructure acts as a standards-based messaging middleware between service access providers and government departments acting as service providers. Additionally, for mobile governance services, Mobile Service Delivery Gateway (MSDG) has been created that provides a government-wide shared infrastructure.
Mobile Governance (m-Governance)

m-Governance (Mobile Governance) aims to leverage wireless and new media technology platforms, mobile devices and applications for delivery of public information and services to all citizens and businesses. It aims at widening the reach of, and access to, public services to all citizens in the country, especially in the rural areas by exploiting the much greater penetration of mobile phones in the country.

It also leverages the innovative potential of mobile applications in providing public services. The overall strategy aims at making India a world leader in harnessing the potential of mobile governance for inclusive development.

The initiative has been conceptualized and formulated by the Department of Electronics and Information Technology (DeitY), Government of India. Centre for Development of Advanced Computing (C-DAC), a DeitY organization, is the technical implementing agency for the project.

Mobile Seva

Mobile Seva is an innovative initiative aimed at mainstreaming mobile governance in the country. It provides an integrated whole-of-government platform for all Government departments and agencies in the country for delivery of public services to citizens and businesses over mobile devices using Short Message Service (SMS), Unstructured Supplementary Service Data (USSD), Interactive Voice Response System (IVRS), Combined Braking System (CBS), Linked Braking System (LBS), and mobile applications installed on mobile phones.

The image below shows the various components of Mobile Seva:
Fig. 4.17: Various components of mobile Seva

The users can access different mobile applications from the website https://apps.mgov.gov.in/index.jsp.
**e-Mail System**

Email is a communications tool that allows individuals to send, receive, and save messages on their computer. There are different e-mail programs available in the market which helps the users to send and receive mails easily. Each email program is slightly different, but they all do basically the same thing: send and receive mail and attachments. There are two basic variations of email programs:

1. A Web interface (or Internet email), such as Yahoo Mail or Gmail:
   - The email software is a special Web interface on the Web mail server. It requires a separate username and password required to access the email. The mail can be accessed from any computer with Internet access.

2. Client software (or network email), such as Microsoft Outlook or Lotus Notes etc.:
   - The email client software resides on each individual's network computer. The email server is located in the same network where the individual computers are on. It requires a separate username and password required to access the email. In some network setup, the username password may not be required. The mail can be accessed from any computer which has the client with Internet access.

![Figure 4.18: Google Gmail Account](image)

**E-Mail Views**

The email application screen is divided into different panes so that users can access the mails easily. These include:
• **Preview pane**: Another way of looking at a message. Instead of double-clicking a message to open it, you can read the message appear in the preview pane.

• **Folder pane**: Various folders, including Sent Items, Trash, and Drafts folders, contain messages that you have sent to other individuals, deleted, or messages you started to write but decided to send later.

### Read New Email

To read email:

1. Locate the Inbox and look for the new mails in the Inbox.
2. Click on the hyperlink of the new mail to open it.

### Send Email

To create a new mail, click on the **Compose Button** on the e-mail website or New option in any of the e-mail client application. A new page will open as shown in the figure below:

![Fig. 4:19: Compose a message](image)

The user needs to provide certain information to send a mail:

1. **Email Addresses**: An email address is made up of three parts, the user name, @ sign and the domain name. For example, an email address "an email address "john.joe@gmail.com" contains few elements, such as "john.joe" as the user name, @ is to differentiate the username and the domain name, and "gmail.com" is the e-mail provider’s name. The e-mail ID needs to be added in the To text box provided in the application.

2. **CC** text box: CC means "Carbon Copy". The e-mail address listed in the CC field of a message gets a copy of that the message sent by the user. Other
recipients of the e-mail message can see that the e-mail ID you designated as a Cc: received a copy of the message sent.

3. **BCC text box**: BCC means "blind carbon copy." Almost similar to the CC, except that Bcc: recipients are invisible to all the other recipients of the message.

4. **Attachments**: Email programs allow the user to send files as a link with the mails to other recipients. Email program helps the user to add more than one file with a single message as attachments.

5. **Subject**: The user should write a Subject in this text field to signify the summary of the mail which is been sent.

6. **Message filed**: Here, the user will type the message for the recipient.

Once the message is completed, the user can click on the **Send** button to send a message to the recipient. Once the message is sent, it is automatically moved to **Send mail** folder. User can view the message by clicking on the **Sent mail** folder listed at the left side of the screen.

**Instructions for New e-Mail User Registration in Government of India domain**

- Users can log into [https://mail.gov.in](https://mail.gov.in) for accessing the webmail portal.

- If you are a government employee (central or state) you can take a @Gov.in id. This id will be assigned to you at no cost.

- Individuals can fill up the single user form. State/Ministries/Departments can fill out the bulk user form if they wish to get multiple number of user's under their domain. Application form should be complete in all respect.

- Submit the filled application form to your respective NIC Coordinator in the NIC cell in your respective State/Ministry/Department.

- If you have a website of your respective department and wish to get the id's created as userid@(website name), the same can be assigned to you.

- Accounts will be created as per the availability of the preferred Email ID. In case the preferred Email id is not available, NIC will assign the id as per the Email address policy.

- The credentials will be sent to registered mobile number of the user.

- When the user logins for the first time, an update "profile page" will be shown. Users are requested to kindly fill the same.
• User will be required to change the password on the first login. Please follow the password policy due to security reasons.

**Limits at Mail Gateways**

• All outgoing and incoming mails from and to NICNET shall enter and leave the Network through the SMTP Gateway.

• All mails, incoming/outgoing will be checked for virus and possibility of Spam.

• Anti-relay options will be enabled on all mail servers. Servers configured as open-relay shall be disconnected from the Network, without any warning.

• All servers in NICNET are configured for a Maximum of 16 MB message size (this includes message header, all attachments encoded into printable ASCII characters) only.

• Mails will stored at the SMTP gateways for a period of 5 days only. Mails not delivered within 5 days will be deleted from the gateway.

**Limits for Mail Clients**

• Max recipients allowed per mail are 50.

• Max message size can be attached using Outlook Express/WEB browser to the mail is 8MB.

• Maximum size of a decompressed file is 40MB

• Max decompressed file count (maximum number of files in a zipped archive send along with the e-mail as attachment) is 100

• Maximum no of attachments is 50

• Mailboxes of users occupying more than 70 MB in their INBOX will be deleted. Users are advised to move important mails to a folder. Restoration requests will NOT been trained.
e-Mail: Dos and Don’ts

- Avoid exposure of E-Mail account details such as user name and password to unknown/unauthorized persons while using E-Mail.

- Avoid unauthorised disclosure of email contents to protect privacy of information

- Avoid clicking of web-links provided in email messages to prevent secretly installation of a malware (e.g., virus) on your computer

- Install latest Anti-virus/Anti-Spyware software and keep them up-to-date.

- Install personnel (Desktop/user level) Firewall on the system.

- Keep Operating System and application software updated with latest security updates/patches in the computer system used for email to prevent the exploitation of the weakness in the system.

- Be suspicious while opening unexpected emails.

- Do not open suspicious email Attachments.

- Scan an email attachment before opening/downloading to minimize the risk of downloading malware (e.g., virus).

- Use encryption for sending and receiving confidential email to ensure that message can only be read by the intended recipients.

- Do not respond suspicious/banking-related (Phishing)/winning lottery/fund transfer emails to avoid becoming a victim of financial frauds.

- Do not open untrusted/unknown emails (spam)

- Enable spam filter to reduce amount of spam/junk emails

- Keep strong password with minimum of eight characters, comprising a combination of alphabets (both upper and lowercase), numbers and special-characters.

- Do not keep your computer unattended to avoid misuse
Chapter Summary

- e-Governance is refers to managing the Government’s activities using information and communication technology (ICT).
- National e-Governance Plan (NeGP) is a plan of the Government of India to make all government services available to the citizens of India via electronic media.
- Mission Mode Projects (MMPs) are individual projects within the National e-Governance Plan (NeGP) that focus on one aspect of electronic governance, such as banking, land records or commercial taxes etc.
- The National e-Governance Plan (NeGP) of the Govt. of India aims to make all Government services accessible to the common man in his locality, through common service delivery outlets and ensure efficiency, transparency & reliability of such services at affordable costs to realize the basic needs of the common man.
- The Government has approved the Scheme for establishing State Wide Area Networks (SWANs) across the country. Under this Scheme, technical and financial assistance are being provided to the States/UTs for establishing SWANs to connect all State/UT Headquarters up to the Block level via District/sub-Divisional Headquarters, in a vertical hierarchical structure with a minimum bandwidth capacity of 2 Mbps per link.
- State Data Centre (SDC) has been identified as one of the important element of the core infrastructure for supporting e-Governance initiatives of National eGovernance Plan (NeGP).
- Assam Electronics Development Corporation Ltd. (AMTRON) has been designated as the State Level Agency of Government of Assam for the implementation of various state-level and national-level projects. These are namely, ARBAS, ASWAN, CSC, SDC, etc.
- Electronic Authentication (or “e-Authentication”) is the process of electronic verification of the identity of an entity.
- The e-Pramaan framework enables various government departments and agencies to address the access management and authorisation requirements associated with the deployment of e- governance applications and services.
- m-Governance(Mobile Governance)aims to leverage wireless and new media technology platforms, mobile devices and applications for delivery of public information and services to all citizens and businesses.
Exercises

1. What do you understand by e-Governance?

2. What is Mission Mode Projects (MMPs)?

3. What is National e-Governance Plan (NeGP)?

4. What is State Data Centre (SDC)?

5. Explain e-Pramaan framework.
Chapter 5

e-District Project

Chapter Objectives:

Districts are the front-end of Government where most Government-to-Citizen or G2C interaction takes place. The e-District project was conceptualized to improve this experience and enhance the efficiencies of the various Departments at the district-level to enable seamless service delivery to the citizen. This chapter gives an overview to the e-District project of Govt. of India.

Chapter in a Nutshell:

E-DISTRICT PROJECT

OBJECTIVE OF THE E-DISTRICT PROJECT

SERVICE TYPE AS DEFINED IN THE NATIONAL ROLL OUT

- TYPE 1 SERVICES
- TYPE 2 SERVICES
- TYPE 3 SERVICES
- QUALITY OF SERVICE
- SERVICE LEVEL

E-DISTRICT DEPLOYMENT FRAMEWORK

- FUNCTIONAL ARCHITECTURE
- INSTITUTIONAL FRAMEWORK ENVISAGED

FRAMEWORK OF DEGS

- APPROVAL OF CABINET
- OBJECTIVES OF THE DEGS
- GOVERNING BODY
- FUND PROVISIONS
- CAPACITY BUILDING

E-DISTRICT PROJECT IN ASSAM

- SERVICES OFFERED THROUGH ASSAM E-DISTRICT PROJECT
- SOME KEY LEARNING OF THE PILOT
- SERVICE DELIVERY MECHANISM
- PROJECT IMPLEMENTATION
The e-District Project

The e-District project was conceptualized and approved in the year 2011 with the intention of creating an enabling environment and a platform for design, development and maintenance of applications relating to various departments and for providing of services to the citizens, at the district and sub-district levels. e-District is one of the 27 MMPs under NeGP, which is being implemented by Department of Electronics and Information Technology (DeitY), Government of India (GoI) as the nodal department at central level through the Information Technology Departments of all States. The project will cover all the districts of the country.

Objective of the e-District Project

The objectives of the e-District Mission Mode Project are to ensure the following:

a. Undertake backend computerization of district, SDO, Circle level offices to ensure electronic delivery of high volume citizen centric services at the district level.

b. Efficient delivery of services with improved service levels by undertaking extensive Business Process Re-engineering (BPR) of identified services.

c. Extensive capacity building and training of field level functionaries to ensure smooth migration to electronic delivery of e-district services and phasing out manual delivery of services.

d. Delivery of services through CSCs by leveraging the common infrastructure of SWAN, SDC, and SSDG.

e. Development of applications to be hosted at the SDCs for delivery of services.

f. Providing easy, anywhere and anytime access to government services (both information & transactional) to ensure reliability, efficiency, transparency and accountability.

g. Reducing number of visits of citizens to a government office / department for availing the services and thereby eliminating harassment.

h. Reducing administrative burden and service fulfillment time and costs for the government, citizens & businesses.

i. Reducing direct interaction of citizen with the government and encourage ‘e’-
interaction and efficient communication through portal.

j. Enhancing perception & image of the Government and its constituent Departments. Prior to National Level roll out of the project, DeitY, GoI had conducted the pilot in 41 districts across the country and based on the learning from the pilot, the frame work for National Level roll out of the project has been designed and with following key points

**Integrated Framework (CSC, SDC, SWAN and SSDG)**

- **Ensuring the optimal use of Infrastructure**: The objective is to optimally leverage the infrastructure created in the form of SDC, SWAN, SSDG, CSC and the other ICT infrastructure created by the State under various initiatives and harmonize it with the e-District MMP.

- **Making e-District project service-oriented and transaction-oriented**: Success of any MMP will be measured in terms of number of G2C transactions delivered per month across all services in the portfolio.

- **Rapid Roll out Approach**: Every State/UT should aim to take advantage of the successful implementation of applications that have become fully mature in other States or have been successfully implemented on a pilot basis within the same State. The effort should be to quickly dovetail such identified applications with the e-District project, of course, with suitable customization, and plan for their quick rollout throughout the State. These will also **Minimize the Time to Benefit** in terms of compressing the project timelines from conceptualization to completion, to deliver all the selected services across the entire State.

- **Common recommended architecture**: Designing the right architecture is the key to success in the e-District rollout. This would enable integration of the applications and delivery of e-Services in an efficient, secure and integrated manner, in the fastest

- **State and district level support**: Deployment of State Project Management Unit and District level Project Manager under the project to help both the State Government and District Administration.

- **Formation of District e-governance society**: In order to manage the project successfully and sustain the project, DeGS have been planned to form in all District. The committee will be chaired by Deputy commissioner

- **Service Focus in the e-District**: The e-district project focuses mainly on the high volume citizen centric service delivery and accordingly Five service categories have been identified at the national level which shall be taken up
for implementation by all States:

a. Issue of Certificates including services: Birth, Death, Domicile, Nationality, Caste, Marriage, Income, Employment, etc.


c. Revenue Court including services – including Case listing, Case adjournment, Stay orders, Final orders, Status of execution of orders: information, tracking, filing of miscellaneous applications. Also, Government dues and recovery, as part of Land Revenue – including issue of notices, record payments, and track default processes, updation of treasury receipts, etc.

d. Ration Card related services including change of address, addition or deletion of members, application for issue of duplicates, etc.

Three additional categories of services identified at the State level are given below:

- Right To Information (RTI) Services
- Electoral Services
- Employment

States has selected different number of services under each category. However, there are some common high volumes Government to Citizen Services selected by all the States. Each State has re-engineered these services within the boundaries of respective legal framework and maturity of ICT in the state.

**Service Type as Defined in the National Roll Out**

The States / UTs should prioritize the citizen services which can be provided immediately to the citizens. The focus should be on services that can be delivered across the counter so citizen does not have to visit a service delivery access point multiple times. The services are categorized as follows:

**Type 1 Services**

These are the services that can be provided “instantaneously” across the counter. These services would be those where an accurate digital database is available, for example the database of Land Records, Transport etc. Further it is also possible that once births and deaths are registered, and are stored in a secured database and digitally signed and thereafter these services can be provided on demand. The provision
of statutory services across the counter, like a variety of certificates, requires that the
database is digitally signed by the competent authority in bulk in advance, such that
when any citizen makes a request, the relevant record is downloaded and a certificate
can be issued by the CSC agent.

**Type 2 Services**

These are those services which require a minimum of 2 visits, but can migrate to Type 1
services with due data digitization, onetime physical verification and digital certification.

**Type 3 Services**

These services require physical presence of the citizen / verification / inspection and
cannot be delivered across the counter e.g. issues of driving license, sub-division of
land, etc.

**Quality of Service**

The quality of an e-Service depends on the manner of its delivery. In some projects,
despite the launch of the ‘e-Service’, the following practices are noticed:

a. the citizen has to make a number of trips to the Government office;
b. the citizen is not sure when the service would finally be delivered;
c. there is a significant dependency on the age-old back-end processing, use of
discretion, avoidable inspections etc. Such services as above do not merit to
be called e-Services, and cannot be included in such a form in the portfolio of
e-District.

The following attributes, in the descending order, qualify a true e-Service:

a. The service can be availed by the citizen over the Internet or mobile, on a
   self-service basis, and on a 24x7 basis;
b. The service can be availed Across-the-Counter in any designated kiosk;
c. The service can be availed with complete certainty on the delivery time;
d. Where physical contact is a necessary part of the delivery system, the service
   centre has the right ambiance and amenities for the citizen’s convenience.
e. The same service can be availed equivalently at a number of delivery points,
   like service centers, kiosks etc.

**Service Level**

While delivering the e-services, key emphasis has to be provided to the improvement in
the service levels. The e-District project has stressed on delivery of the service with a
clear commitment on achieving acceptable service levels for the services selected.
Already some States have Service Delivery Guarantee Acts which provide for delivering
services within a stipulated time and also provisions to impose penalty on the concerned officer in case the service levels are not met.

**Note:** RTPS Act, 2013 of Assam guarantees delivery of services to the citizen in time bound manner for number of services notified under the Act.

There shall be a clear emphasis on the service levels for each service being provided to the citizens. Service levels seek to guarantee the time period in which the service shall be delivered to the citizen and the quality thereof. Adoption of well-defined service levels enhances the citizen satisfaction, besides placing enforceable contractual obligations on the service providers, through the relevant Service Level Agreements.

**e-District Deployment Framework**

The e-District architecture envisages leveraging of the core NeGP components of State Wide Area Network (SWAN), State Data Centre (SDC), State Services Delivery Gateway (SSDG) and Common Services Centres (CSCs). Applications and data under e-District project are to be hosted at the SDC and all field offices are to be connected through the SWAN. Those horizontal offices which are required to be connected for the delivery of services and are not already connected to the SHQ, DHQ or BHQ under the SWAN project are to be provided horizontal connectivity under e-District project. Citizens will access services through the Common Services Centres and no separate physical front ends for delivery of services have been envisaged under the e-District project.

The e-District project has planned to leverage the middleware in the form of State Services Delivery Gateway. In States where SSDG is operational, e-District should integrate with the SSDG and necessary e-form for all services to be hosted in the State Portal. The SSDG project connects with the e-District application for end to end integration.
Functional Architecture

A Functional Architecture is a logical representation of:

(i) the business functionalities that an organization wants an IT-based system to deliver and of

(ii) the manner in which the various categories/classes of users interact with the system. In the context of the e-District Project, the following elements enable designing of an appropriate:

a) **Citizen Interfaces**: It is expected that the e-District services would be accessed by the citizen through various channels. At the minimum the citizen would be accessing the services from the CSCs. The Citizens should also access the services directly by accessing the web portal or through mobile devices. However, both the citizens and CSCs, will access the web-portal for availing the services. This web portal should be the State Portal (preferred) or e-District portal or both.

b) **Department Interfaces**: The departments at the backend need to access the system for various purposes like data entry, data updation, approvals through workflow etc. These interfaces can be via the Internet or through an Intranet.

c) **Basic functional elements**: The e-District service delivery demands 24x7 availability of the system, authentication and authorization of various classes of users, workflow system for approvals, digital signature/PKI for authenticating records/certificates, payments to be made, MIS, Dashboards for monitoring and mobile services.

The e-District Business layer should, inter alia, provide for:
a) Workflow, for facilitating approvals at various levels while processing a citizen request.
b) Authentication of the citizen through Aadhaar
c) PKI Support for facilitating the usage of digital signatures
d) Payment Gateways, to make the payments directly by using credit/debit cards.
e) Mobile services for communicating the updates to the citizen

Institutional Framework Envisaged

![Proposed Institutional Framework]

Fig. 5.2: Proposed Institutional Framework

Framework of DeGS

District e-Governance Societies (DeGS) are envisaged to play the role of nodal agency to manage, supervise and implement the various e-Governance projects in the Districts. Since a number of projects are being implemented at the District and sub-District level, DeGS is required to be formed in each District for supervision, management, hand-holding and coordination of project activities. The DeGS shall play an important role in the successful implementation and maintenance of the various e-Governance projects in the Districts.

Approval of Cabinet

To ensure alignment of objectives and functions across all the DeGS formed in the State, the Memorandum of Association and Rules of the Society were approved by the Cabinet vide endorsement dated 09/09/13 by Political (Cabinet Cell) Department in File
No. IT. 104/2010/Pt II. Henceforth, it was mandated that the DeGS formed in each District shall have to adopt the Memorandum of Association and Bye Laws as approved by the Cabinet.

**Objectives of the DeGS**

1. To roll out and maintain e-District application and other electronic citizen services in the district, and other e-governance projects in the Districts;
2. To manage, supervise and implement back-end computerization of Government Departments;
3. To assist in undertaking the field work, comprehend the requirements, document the observations and prepare road-map;
4. To build capacity of the staff and executive resources of the district administration;
5. To implement guidelines of State Government and Government of India for e-District, CSC, SWAN, SDC, SSDG and any other e-Governance Programmes in the District;
6. To support the Common Services Centers (CSCs) in the District for providing G2C/ G2B services, to identify and recommend the Citizen Services which can be provided through CSCs and assist SCA in roll out of services in CSCs;
7. To collect user charges, share revenue with approved stakeholders and collect statutory dues;
8. To take suitable publicity measures and awareness campaign through any media for creating awareness about transformation through e-Governance for the benefit of the citizens;
9. To maintain the infrastructure under any e-governance project after the expiry of the contract period with the Implementing Agency and devise appropriate strategy in consultation with the SDA to ensure sustainability of such project;
10. To undertake any other function as may be assigned by the State Government, Government of India, Department or the SDA;

The Society functions under the control of the State Government. All functions of the society should be in line with the policies, frameworks, etc. of the Government of India and State Government. The State Government shall have absolute and overriding power in respect of appointment, change and removal of members as also in formation of Committees and Sub-Committees under the Rules. The activities and accounts of the Society shall always be open for verification by the Government or the Comptroller and Auditor General. The State Government and IT Department, shall have the power to issue such directions/instructions as may be deemed necessary for proper functioning of the Society.
**Governance Body**

Except the Co-opted members, the constitution of the Governing body is same as the General Body. The Deputy Commissioner is the Chairman and the Additional Deputy Commissioner (Development) is the Member Secretary. The Governing body is primarily for looking after administrative matters, implementing the policy decisions of the General Body and conducting business and affairs of the Society. The Member Secretary of the Society is in overall charge for keeping the records of the Society including accounting books, minutes in order, day to day matters.

**Fund Provisions**

Each DeGS will be provided with an amount of Rs. 10 lacs as seed money under the project.

The DeGS are mandated to collect user charges as fixed by the State Government and keep audited accounts of the same. All fund should be applied for the promotion of objects of the State.

**Capacity Building**

To achieve the above, necessary Capacity Building measures are adopted and some of the steps planned within the e-District Scheme apart from Training of the staff of district administration are as follows:

a) **State Project Management Unit**: The State Project Management Units have been selected centrally by DeitY and these agencies should help the IT Department/SDA in development of the Scope of work, selection of SI for implementation of the project, BPR finalisation, training plan development and monitoring of the project etc.

b) **State e-Governance Mission Teams**: The SeMTs should be tasked to interact with the line Department of State Departments to get their support for the e-District project. They should ensure consistency between the State specific technical architecture and e-District Technical architecture. In case of any variance between the two, there should be a roadmap so that the consistency is ensured within a timeline.

c) **e-District Managers**: The role of e-District Manager would be critical in making the project a success. The e-District Manager will be responsible for project management & co-ordination at a district level. He also will play an instrumental role in training the district level officials in delivering services within the specified service levels.
d) **District e-Governance Societies**: Formation of District e-Governance Societies (DeGS) and institutional capacity building through DeGS would be instrumental. It may be noted that all the district level funds will be transferred to the DeGS and this would provide the flexibility to the DC/DMs in managing the e-District project’s day-to-day affairs at the district level. The detail of the DeGS has already been mentioned.

### e-District Project in Assam

Assam was one of the 14 states in the country, where the e-District imitative was planned as "Pilot" project. The Government of Assam has chosen two districts, Sonitpur and Goalpara for the pilot implementation of the project. The districts of Goalpara had gone live in the month of November’2009 and Sonitpur in January’2010.

### Services Offered through Assam e-District Project

The services indicated below are covered under Assam e-District (Pilot) Project.

**Certificates**
- 1 Permanent Residence Certificate
- 2 Senior Citizen Certificate
- 3 Next of Kin Certificate
- 4 Non-Creamy Layer Certificate
- 5 Land Valuation Certificate
- 6 Bakijai Clearance Certificates
- 7 Income Certificate

**Permissions**
- 1 Permission for Delayed Birth Registration
- 2 Permission for Delayed Death Registration
- 3 Permission for Special Events U/s 144 CrPC

**Certified Copies**
- 1 Certified Copy of Electoral Roll
- 2 Certified Copy of Mutation Order

**Others**
- 1 Grievance
- 2 Jamabandi for Surveyed Villages

**Pensions**
- 1 National Old Age Pension Scheme
- 2 National Family Benefit Scheme

**FIC**
- 1 Family Identity Card
For the state wide roll out, five services are identified.

1. Permanent Residence Certificate
2. Non Creamy Layer Certificate
3. Next of Kin
4. Permission for Delayed Death Registration
5. Permission for Delayed Birth Registration.

**Some Key Learning of the Pilot**

The pilot experience of the project was a mixed one and service delivery did not took place as expected because of the following few reasons:

   a. Non availability of reliable connectivity
   b. Frequent power cut and damage of the UPS
   c. Lower level of Public awareness about the project
   d. Effective BPR of the services
   e. Non-adherence to service level etc.

Despite all these more than 1 lakh online services were delivered and certificates were issues signing digitally. The key learning from the project will be useful for the State wide roll out.
Chapter 5: e-District Project

Proposed Service Delivery Mechanism

<table>
<thead>
<tr>
<th>Citizen</th>
<th>CSC/ PFC Operator</th>
<th>Back End Operation</th>
<th>CSC/ PFC Operator</th>
<th>Citizen</th>
</tr>
</thead>
<tbody>
<tr>
<td>Goes to CSC or PFC and makes service request</td>
<td>Receives the application, logs into State Portal and forwards the application</td>
<td>Logs into e-District portal, views the application, processes the same, digitally approves/rejects &amp; send back to CSC/ PFC Operator</td>
<td>Received the requested service through State Portal and deliver to the citizen OR Does the necessary correction(s) and forward the application again to the authority</td>
<td>Receives the service from the CSC/ PFC Operator</td>
</tr>
</tbody>
</table>

Step: 1 The citizen comes to the CSC/ PFC and requests the operator to submit his/ her application.

Step: 2 The CSC/ PFC operator logs in to the State Portal and submits the application. After submission the application automatically routes to the concern official.

Step: 3 The application lands up in the inbox of the concern officer, the officer sends the same to his subordinates for further actions. After completion of due process, the application comes back to the issuing authority. Once satisfied, viewing the complete proceeding of the application, the authority may deliver the service by appending his/ her digital signature. Otherwise he/ she may also send back to subordinates for further actions or revert back to the CSC/ PFC operator for correction or reject the application. This entire operation happens in the e-District application and all the users need to log in to the system using user ID, password and biometric authentication.

Step: 4 The CSC/ PFC operator logs in to the State Portal and takes out the printout and deliver the same to the citizen. If the application is reverted back for further correction, the operator incorporates the same into the application and submits again.
Step: 5  The citizen receives the services from the CSC/ PFC Operator.

**Project Implementation**

The project is being implemented across the 27 district in the State covering all DC offices, SDO and Circle offices Necessary notification for DeGS formation has already been published and appointment of District Project Manager are also going on. The following key activities have been planned project covers mainly five aspects:

a. Site Preparation  
b. IT Hardware  
c. State Data Centre Hardware  
d. Software Development and Maintenance  
e. Training and Capacity Building  
f. Digitation of legacy records  
g. Awareness and communication plan for the citizen

1. **Site Preparation**: For efficient management of service delivery under e-District project, site preparation activity needs to be completed across the concerned offices. This requires making the office space prepared for deployment of ICT infrastructure. Site preparation covers Electrical and LAN Connectivity as well as Civil and Mechanical works to safeguard the hardware supplied. Adequate safety measures have to be taken at all the locations.

2. **IT hardware deployment plan:**

<table>
<thead>
<tr>
<th>Equipment</th>
<th>DC Office</th>
<th>DCO -FC</th>
<th>SDO ( C )</th>
<th>SDO( C ) - FC</th>
<th>Circle Office</th>
<th>CO - FC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop</td>
<td>24</td>
<td>6</td>
<td>16</td>
<td>4</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>Laptop</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>MFP</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Laser Printer</td>
<td>6</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>UPS</td>
<td>24</td>
<td>6</td>
<td>16</td>
<td>4</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>Biometric</td>
<td>24</td>
<td>6</td>
<td>16</td>
<td>4</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>DG-5 KVA</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>DG-10 KVA</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

*Actual figure may vary*
The capacity building program under the project envisages to enable the officials/staff working in the district administration to cope up with necessary changes with the deployment of ICT assets in their day to day working as well as delivery of electronic services in time bound manner.

<table>
<thead>
<tr>
<th>Sr No</th>
<th>Training Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Basic Computer Training</td>
</tr>
<tr>
<td>2</td>
<td>Specialized Computer</td>
</tr>
<tr>
<td>3</td>
<td>E-District Application Training</td>
</tr>
<tr>
<td>4</td>
<td>e-District Process training</td>
</tr>
<tr>
<td>5</td>
<td>Usage of Digital Signature</td>
</tr>
<tr>
<td>6</td>
<td>Filling of Application (VLE)</td>
</tr>
</tbody>
</table>

**Chapter Summary**

- e-District is one of the 27 MMPs under NeGP, which is being implemented by Department of Electronics and Information Technology (DeitY), Government of India (GoI) as the nodal department at central level through the Information Technology Departments of all States.

- The States / UTs should prioritize the citizen services which can be provided immediately to the citizens.

- The e-District project has planned to leverage the middleware in the form of State Services Delivery Gateway.

**Exercises**

1. Explain objectives of the E-district project?
2. What do you mean by rapid roll out Approach?
3. Describe e-District Deployment Framework.
4. What is roll of DeGS in district level?
5. Explain e-District project plan in Assam state.
Chapter 6

Introduction to IT Security Policy

Chapter Objectives:

The electronic transaction which happens in the cyber space has been increasingly facing security threats of different nature. In order to prevent increasing cybercrime and protect the system and resources in use from such security threats, the IT Security today considered as an important factor by all the Governments, Business houses and the common citizen. Years of critical data, personal information and sensitive documents can be lost or destroyed without a plan for securing them and a good IT Security plan. This chapter provides an overview of IT Security policy adopted by the country.

Chapter in a Nutshell:

CYBER CRIMES: LAW AND PRACTICE
IT SECURITY POLICY
THE INDIAN CYBER SPACE
THE INFORMATION TECHNOLOGY (IT) ACT 2000
NATIONAL CYBER SECURITY POLICY 2013
INFORMATION SECURITY POLICY FOR ORGANIZATIONS
Cyber Crimes: Law and Practice

Cybercrime means any criminal activity in which a computer or network is the source, tool or target or place of crime. The Cambridge English Dictionary defines cybercrimes as crimes committed with the use of computers or relating to computers, especially through internet.

Crimes involving use of information or usage of electronic means in furtherance of crime are covered under the scope of cybercrime. Cybercrimes may be committed against persons, property and government. The common types of cybercrimes may be discussed under the following heads.

1. **Hacking**: A hacker is an unauthorized user who attempts to or gains access to an information system. Hacking is a crime even if there is no visible damage to the system, since it is an invasion into the privacy of data. There are different classes of Hackers.
   a. **White Hat Hackers** - They believe that information sharing is good, and that it is their duty to share their expertise by facilitating access to information. However there are some white hackers who are just “joy riding" on computer systems.
   b. **Black Hat Hackers** - They cause damage after intrusion. They may steal or modify data or insert viruses or worms which damage the system. They are also called ‘crackers’.
   c. **Grey Hat Hackers** - Typically ethical but occasionally violates hacker ethics. Hackers will hack into networks, stand-alone computers and software. Network hackers try to gain unauthorized access to private computer networks just for challenge, curiosity, and distribution of information. Crackers perform unauthorized intrusion with damage like stealing or changing of information or inserting malware (viruses or worms).

2. **Cyber Stalking**: This crime involves use of internet to harass someone. The behavior includes false accusations, threats etc. Normally, majority of cyber stalkers are men and the majority of victims are women.

3. **Spamming**: Spamming is sending of unsolicited bulk and commercial messages over the internet. Although irritating to most email users, it is not illegal unless it causes damage such as overloading network and disrupting service to subscribers or creates .negative impact on Consumer attitudes towards Internet Service Provider.

4. **Cyber Pornography**: Women and children are victims of sexual exploitation through internet. Pedophiles use the internet to send photos of illegal child pornography to targeted children so as to attract children to such fraud. Later they are sexually exploited for gains.
5. **Phishing**: It is a criminally fraudulent process of acquiring sensitive information such as username, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.

6. **Software Piracy**: It is an illegal reproduction and distribution of software for business or personal use. This is considered to be a type of infringement of copyright and a violation of a license agreement. Since the unauthorized user is not a party to the license agreement it is difficult to find out remedies.

7. **Corporate Espionage**: It means theft of trade secrets through illegal means such as wire taps or illegal intrusions.

8. **Money Laundering**: It means moving of illegally acquired cash through financial and other systems so that it appears to be legally acquired. Transport cash to a country having less stringent banking regulations and move it back by way of loans the interest of which can deducted in the form of taxes. This is possible prior to computer and internet technology came into existence. Today, electronic transfers have made it easier and more successful.

9. **Embezzlement**: Unlawful misappropriation of money, property or any other thing of value that has been entrusted to the offender’s care, custody or control is called embezzlement. Internet facilities are misused to commit this crime.

10. **Password Sniffers**: Password sniffers are programmes that monitor and record the name and password of network users as they log in, jeopardizing security at a site. Whoever installs the sniffer can impersonate an authorized user and log in to access on restricted documents.

11. **Spoofing**: It is the act of disguising one computer to electronically “look” like another compute, in order to gain access to a system that would be normally is restricted. Spoofing was used to access valuable information stored in a computer belonging to security expert

12. **Credit Card Fraud**: In U.S.A. half a billion dollars have been lost annually by consumers who have credit cards and calling card numbers. These are stolen from on-line databases.

13. **Web Jacking**: The term refers to forceful taking of control of a web site by cracking the password.

14. **Cyber terrorism**: The use of computer resources to intimidate or coerce government, the civilian population or any segment thereof in furtherance of political or social objectives is called cyber terrorism. Individuals and groups quite often try to exploit anonymous character of the internet to threaten governments and terrorize the citizens of the country.
### IT Security Policy

Cyber Security is of major concern in today’s era of computing to secure data, network resources, and other critical information of any organization. Cyber security is now not restricted only affects the usage of Internet on a Desktop PC but also securing information on Tablets, smart phones as they became very important communication medium because of technological advancements grown up very rapidly in past few years.

According to emerging cyber threat report 2014 of Georgia Institute of Technology mobile devices bring a new set of threats, including allowing malicious software. Mobile platforms have largely been safe for consumers and businesses, researchers and attackers are finding ways around the eco systems security. According to IC3report 2012 (Internet Crime Complaint Centre) an alliance between the National White Collar Crime Centre (NW3C) and Federal Bureau of Investigation (FBI) the top five countries by count in victim complaints as numbered by Rank) as follows:

![Fig. 6.1: Top five countries affected by cyber crime](image)

### The Indian Cyber Space

The rapid development of the Internet over the past decade appeared to have facilitated an increase in the incidents of Online attacks In India National Informatics Centre’s were setup in year 1975 to provide various IT related solutions to the government. There were three major networks were setup at that time.

- Critical sectors such as Defense, Energy, Finance, Space, Telecommunication, Transport and other public services heavily depends on the network to relay data, for communication purpose and for commercial
transactions.

- These sectors have a large impact of using the Internet as a source of communication, and information
- National broadband plan the target for broadband is 160 million households by 2016 and the Networking index estimates that India’s Internet traffic will grow nine-fold between now and 2015.
- The government has ambitious plan to raise cyber connectivity, ecommerce services and communication channel.

The Information Technology (IT) Act 2000

In India the Information Technology Act 2000 was passed to provide legal recognition for transactions carried out by means of electronic communication. The Act deals with the law relating to Digital Contracts, Digital Property, and Digital Rights Any violation of these laws constitutes a crime. The Act prescribes very high punishments for such crimes. The Information Technology (amendment) Act, 2008 (Act 10 of 2009), has further enhanced the punishments. Life imprisonment and fine upto rupees ten lakhs may be given for certain classes of cybercrimes. Compensation up to rupees five crores can be given to affected persons if damage is done to the computer, computer system or computer network by the introduction of virus, denial of services etc.(S. 46(1-A)). Sections 65-74 the Act specifically deal with certain offences, which can be called Cyber Crimes

1. Tampering with any computer source code used for a computer, computer programme, computer system or computer network, is punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both. "Computer source code" means the listing of programs, computer commands, design and layout and program analysis of computer resource in any form.

2. Hacking with computer system is to be punished with imprisonment up to three years, or with fine which may extend up to five lakh rupees, or with both.

3. Sending offensive or false information through computer or a communicative device is punishable with imprisonment up to three years and with fine.

4. Receiving or retaining stolen computer resource or communication device is an offence punishable with imprisonment up to three years and fine up to one lakh or with both. The same punishment is prescribed for fraudulent use of electronic signature, password etc. of any other person and for cheating using computer, cell phone etc.

5. Capturing Transmitting or publishing the image of a private area of any person without consent is punishable with imprisonment up to three years and with fine up to two lakhs or with both.
6. Punishment for Cyber terrorism may extend to imprisonment for life.

7. Publishing transmitting information which is obscene in electronic form shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

8. Publication and transmission of containing sexually explicit act or conduct is to be punished with imprisonment up to five years and fine up to ten lakh rupees and for second or subsequent conviction with imprisonment for a term up to seven years and fine up to ten lakh rupees. The same punishment is prescribed for child pornography.

9. Penalty for Misrepresentation whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be. Shall be punished with imprisonment for a term, which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

10. Penalty for Breach of Confidentiality and Privacy; any person who has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

11. Punishment for disclosure of information in breach of contract is imprisonment for a term up to three years or with fine up to five lakh rupees or with both.


(1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that

(a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended, Violation of the above provision is punishable with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. (S. 73)

13. Publication for Fraudulent Purpose.

Whoever knowingly creates publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. In addition to the prescribed punishments, any computer, computer
system, floppies, compact disks, tape drives or any other accessories related to the crime shall be liable to confiscation.

The provision of the Act makes it clear that the provisions of this Act are applicable to any offence or contravention committed outside India by any person irrespective of his nationality if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

**National Cyber Security Policy 2013**

With an aim to monitor and protect information and strengthen defenses from cyber-attacks, the National Cyber Security Policy 2013 was released on July 2, 2013 by the Government of India. The purpose of this framework is to ensure a secure and resilient cyberspace for citizens, businesses and the government. With rapid information flow and transactions occurring via cyberspace, a national policy was much needed.

The policy highlights the significance of Information Technology (IT) in driving the economic growth of the country. Following are the main points covered under this policy:

- It endorses the fact that IT has played a significant role in transforming India’s image to that of a global player in providing IT solutions of the highest standards.
- The Cyber Security Policy aims at protection of information infrastructure in cyberspace, reduce vulnerabilities, build capabilities to prevent and respond to cyber threats and minimize damage from cyber incidents through a combination of institutional structures, people, process, technology and cooperation.
- The objective of this policy in broad terms is to create a secure cyberspace ecosystem and strengthen the regulatory framework.
- A National and sectorial 24X7 mechanism has been envisaged to deal with cyber threats through National Critical Information Infrastructure Protection Centre (NCIIPC).
- Computer Emergency Response Team (CERT-In) has been designated to act as a nodal agency for coordination of crisis management efforts. CERT-In will also act as umbrella organization for coordination actions and operationalization of sectorial CERTs.
- A mechanism is proposed to be evolved for obtaining strategic information regarding threats to information and communication technology (ICT) infrastructure, creating scenarios of response, resolution and crisis management through effective predictive, prevention, response and recovery action.
- The policy calls for effective public and private partnership and collaborative
engagements through technical and operational cooperation.

- The stress on public-private partnership is critical to tackling cyber threats through proactive measures and adoption of best practices besides creating a think tank for cyber security evolution in future.

- It also recommends to for a strategy to promotion the research and development in cyber security by setting up of ‘Centre of Excellence’ in areas of strategic importance.

- The policy also calls for developing human resource through education and training programmes, establishing cyber security training infrastructure through public private partnership and to establish institutional mechanisms for capacity building for law enforcement agencies.

- The policy also aims at encouraging all organizations whether public or private to designate a person to serve as Chief Information Security Officer (CISO) who will be responsible for cyber security initiatives.

- Indian Armed forces are in the process of establishing a cyber-command as a part of strengthening the cyber security of defense network and installations.

- The key to success of this policy lies in its effective implementation. The much talked about public-private partnership in this policy, if implemented in true spirit, will go a long way in creating solutions to the ever-changing threat landscape.

The continuous growth is good for our country but at the same time the government should make strong policies regarding the cyber-attacks and security.

**Information Security Policy for Organizations**

An IT Security Policy is the most critical element of an IT security program. A security policy identifies the rules and procedures that all persons accessing computer resources must adhere to in order to ensure the confidentiality, integrity, and availability of data and resources. In order to follow the Information Security policy for any organization, one has to follow the specific stages as mentioned below:

- Adoption of a security policy
- Security risk analysis
- Development and implementation of a information classification system
- Development and implementation of the security standards manual
- Implementation of the management security self-assessment process
- On-going security programme maintenance and enforcement
- Training.
Chapter 6: Introduction to IT Security Policy

An IT Security Policy is the most critical element of an IT security program. A security policy identifies the rules and procedures that all persons accessing computer resources must adhere to in order to ensure the confidentiality, integrity, and availability of data and resources. An IT Security Policy should contain:

- Communicates clear and concise information and is realistic;
- Includes defined scope and applicability;
- Makes enforceability possible;
- Identifies the areas of responsibility for users, administrators, and management;
- Provides sufficient guidance for development of specific procedures;
- Balances protection with productivity;
- Identifies how incidents will be handled; and
- Is enacted by a senior official with support of top management.

Chapter Summary

- Cyber Security is of major concern in today’s era of computing to secure data, network resources, and other critical information of any organization.

- According to emerging cyber threat report 2014 of Georgia Institute of Technology mobile devices bring a new set of threats, including allowing malicious software.
- There were some major networks were setup at that time, such as; Defense, Energy, Finance, Space, Telecommunication, Transport.
- The government has ambitious plan to raise cyber connectivity, ecommerce services and communication channel.

Exercises

1. What is IT Security Policy?
2. Explain the three major network communications in India?
3. When the National Cyber Security Policy was released?
4. What is the full form NCIIPC?
5. What is the responsibility of CISO?
Chapter 7

The Unique Identification Development Project

Chapter Objectives:

UID project is an initiative that would provide identification for each resident across the country and would be used primarily as the basis for efficient delivery of welfare services. Under UID a 12 digit individual identification number is issued by the Unique Identification Authority of India on behalf of the Government of India which is known as AADHAR. This chapter provides an overview to the services provided by UIDAI. This chapter provides an overview of to the AADHAAR system in India as in future this number may be integrated in most of the G2C services provided by State Government as well.

Chapter in a Nutshell:

THE UNIQUE IDENTIFICATION (UIDAI) PROJECT

WHAT IS AADHAAR?

EVERY INDIVIDUAL IS UNIQUE

Benefits of having a Unique Identity

THE FEATURES OF UID OR AADHAAR

Benefits of AADHAAR for Residents

Benefits of AADHAAR for Government

USE OF AADHAAR

E-AADHAAR
The Unique Identification (UIDAI) Project

Unique identification project was initially conceived by the Planning Commission as an initiative that would provide identification for each resident across the country and would be used primarily as the basis for efficient delivery of welfare services. It would also act as a tool for effective monitoring of various programs and schemes of the Government.

UIDAI’s goal and mission is:

- UIDAI will provide AADHAAR to residents of India that
  - Can be verified and authenticated easily, quickly and in a cost effective way
  - Can eliminate duplicate and fake identities

- In India we already have a huge infrastructure in terms of public and private agencies such as various government departments, banks, insurance companies, oil companies, etc. **UIDAI will use this existing infrastructure to reach out to all sections of the population**

![Fig 7.1: Covering all residents of India](image)

- Although the UIDAI intends to cover all residents of the country, the focus will be on enrolling India’s deprived and marginalized sections. Generally these sections of society do not have any documents to prove their identity. Also, existing identity databases in India like Public Distribution System (PDS), Income Tax, Pension Scheme, etc., may have problems of ‘ghosts’ entries and duplication.

- An AADHAAR will be provided to each individual without putting them through any difficulty or harassing them.
For example, K.S.K Durga, a 45 year old man, died few years ago. Another person named K Durga, 43 years old, assumed the identity of late K.S.K Durga and availed all the benefits for which she was not eligible.

To prevent such errors from getting into the UIDAI database, the UIDAI plans to enroll residents into its database with proper verification of their demographic and biometric information. This will ensure that the data collected is correct from the start of the program.
What is Aadhaar?

- Aadhaar is a 12 digit individual identification number issued by the Unique Identification Authority of India on behalf of the Government of India.

- This number will serve as a proof of identity and address, anywhere in India. Aadhaar letter received via India Post and e-Aadhaar downloaded from UIDAI website are equally valid.

- Any individual, irrespective of age and gender, who is a resident in India and satisfies the verification process laid down by the UIDAI can enroll for Aadhaar.

- Each individual needs to enroll only once which is free of cost.

- Each Aadhaar number will be unique to an individual and will remain valid for life. Aadhaar number will help you provide access to services like banking, mobile phone connections and other Govt and Non-Govt services in due course.

- Aadhaar will be:
  - Easily verifiable in an online, cost-effective way
  - Unique and robust enough to eliminate the large number of duplicate and fake identities in government and private databases
  - A random number generated, devoid of any classification based on caste, creed, religion and geography.

- Aadhaar is:
  - A 12-digit unique identity for every Indian individual, including children and infants
  - Enables identification for every resident Indian
  - Establishes uniqueness of every individual on the basis of demographic and biometric information
  - It is a voluntary service that every resident can avail irrespective of present documentation
  - Each individual will be given a single unique Aadhaar ID number
  - Aadhaar will provide a universal identity infrastructure which can be used by any identity-based application (like ration card, passport, etc.)
  - UIDAI will give Yes/No answers to any identity authentication queries
Every Individual is Unique

When you were born, you probably looked exactly similar to the thousands of babies born at that same instant. After a few months your parents gave you a name, which set you apart from some of those thousands.

But a name alone is not enough for a unique identification. What are the other things that identify you and make you ‘unique’, that is, they set you apart from others?

- Name
- Date of birth
- Gender
- Father's/Husband's/ Mother's/ Wife's/ Guardian's name
- School / College attended
- Address
All the above information can probably be combined to generate uniqueness for you. This information can be verified against various documents as:

- Birth Certificate
- School Leaving Certificate
- Ration Card
- Driving License
- Other similar official documents

However, if such documents do not exist and/or are incorrect, it becomes very difficult to establish an identity. Today, modern technology helps us to record some of the physical attributes, which make each of us different from others. These include:

- **Finger prints**: The lines on the tips of our fingers are unique and can be photographed and stored for future reference. It is an accepted form of identification by various agencies, including our legal system (courts) and financial institutions (banks).

![Fig. 7.5: Finger prints](image)

- **Facial features**: The photograph of our face is one of the most commonly used methods of identification used by various agencies.

- **Iris**: It is a section of the eye which has a unique structure for each person just like the finger print. Today, it is possible to capture the details of the iris for an individual and store it like a photograph for unique identification.

![Fig. 7.6: The Iris](image)
A combination of documents and photograph of physical attributes can be used for a positive and confirmed unique identification.

**Note: Demographic & Biometric Information** - The information related to a person, which can be obtained from official records like name, address, date of birth and so on, are referred to as ‘Demographic’ information. It also includes the information related to nationality, age, education, religion, employment status, and so on. Demographic information is typically collected while filling application forms for passport, ration card, school admission, etc.

The information related to the physical attributes of a person like finger prints, facial features and iris are known as ‘Biometric’ information.

**Benefits of having a Unique Identity**

- You get a bank account, passport, driving license, etc., which no one else has. Your money in the bank cannot be withdrawn by anyone except you.

- You can own a credit card and get a loan.

- You can own a house, a shop or a business.

- If you belong to the marginalized and deprived section of society, the government can help you by providing subsidized food rations and various beneficiary schemes.

**The Features of UID or AADHAAR**

- It will be a randomly generated twelve digit number for every resident of India. Example: 2653 8564 4663. This number will be called the Unique Identification Number or AADHAAR.
• The number will be unique, which means, no two residents will have the same number.

• No resident can have two numbers because AADHAAR is based on a combination of standard information like name, address, age and biometric information which is unique to every person.

• To avoid frauds, the AADHAAR number will have no additional information within its value or structure. It will be a ‘random’ number like the result of a lottery draw or like throwing a dice.

• AADHAR will be used to prove identity not citizenship.

• It will not be compulsory to get an AADHAAR number. It will be voluntary. However in the future, certain service providers (government or private agencies) may require a person to have an AADHAAR number to deliver services.

For example, in future, the Public Distribution System (PDS) department may issue ration cards based on an individual's AADHAAR number and the AADHAAR number will appear in the ration card.

**Benefits of AADHAAR for Residents**

• The AADHAAR will become the single source of identity verification. Once residents enroll, they can use the number multiple times – they would be spared the trouble of repeatedly providing supporting identity documents each time they wish to access services such as obtaining a bank account, passport, driving license, and so on.

• The large number of residents, who currently don’t have any identity documents and are therefore ‘excluded’ from beneficiary lists, can also get an ‘identity’ through the 'Introducer' system. AADHAAR number (or the UID) will thus become the ‘key that opens all doors’ – especially for the deprived and marginalized.

**Benefits of AADHAAR for Government**

Eliminating duplication under various schemes is expected to save substantial money for the government exchequer. It will also provide governments with accurate data on residents, enable implementation of direct benefit programs, and allow government departments to coordinate investments and share information.
Use of Aadhaar

- Universality, which is ensured because Aadhaar will over time be recognised and accepted across the country and across all service providers. Every resident's entitlement to the number.

- The number will consequently form the basic, universal identity infrastructure over which Registrars and Agencies across the country can build their identity-based applications.

- Unique Identification of India (UIDAI) will build partnerships with various Registrars across the country to enroll residents for the number. Such Registrars may include state governments, state Public Sector Units (PSUs), banks, telecom companies, etc. These Registrars may in turn partner with enrolling agencies to enroll residents into Aadhaar.

- Aadhaar will ensure increased trust between public and private agencies and residents. Once residents enroll for Aadhaar, service providers will no longer face the problem of performing repeated Know Your Customer (KYC) checks before providing services. They would no longer have to deny services to residents without identification documents. Residents would also be spared the trouble of repeatedly proving identity through documents each time they wish to access services such as obtaining a bank account, passport, or driving license etc.

- By providing a clear proof of identity, Aadhaar will empower poor and underprivileged residents in accessing services such as the formal banking system and give them the opportunity to easily avail various other services provided by the Government and the private sector.

- The centralised technology infrastructure of the UIDAI will enable ‘anytime, anywhere, anyhow’ authentication. Aadhaar will thus give migrants mobility of identity. Aadhaar authentication can be done both offline and online, online authentication through a cell phone or land line connection will allow residents to verify their identity remotely. Remotely, online Aadhaar-linked identity verification will give poor and rural residents the same flexibility that urban non-poor residents presently have in verifying their identity and accessing services such as banking and retail. Aadhaar will also demand proper verification prior to enrolment, while ensuring inclusion.

- The UIDAI will ensure that it’s Know Your Resident (KYR) standards do not become a barrier for enrolling the poor and has accordingly developed an Introducer system for residents who lack documentation. Through this
system, authorised individuals ('Introducers') who already have an Aadhaar, can introduce residents who don't have any identification documents, enabling them to receive their Aadhaar.

**e-Aadhaar**

Once the Aadhaar status is seen as generated, there is an option to print the Aadhaar from the web site. Click on the link [https://eaadhaar.uidai.gov.in/](https://eaadhaar.uidai.gov.in/) in the Resident Portal to open a window with all relevant details will have to be filled.

1. The enrolment number, date and time of enrolment as given in the acknowledgement slip obtained after enrolling for Aadhaar is required.
2. All details like enrolment number, date, and time of enrolment, name, Pin code and the captcha code are to be filled in the respective fields and Submit button clicked.
3. A valid mobile number will have to be entered / verified and a One Time Password (OTP) will be received on the same mobile number as a part of verification process.
4. This OTP will be needed to proceed further and the OTP has to be entered in the next field to get access to the electronic version of Aadhaar letter or e-Aadhaar card.
5. After that a link to download e-Aadhaar letter (in PDF format) will be provided which can be opened by entering the Pincode as the password.

**Chapter Summary**

- Unique identification project was initially conceived by the Planning Commission as an initiative that would provide identification for each resident across the country and would be used primarily as the basis for efficient delivery of welfare services. It would also act as a tool for effective monitoring of various programs and schemes of the Government.

- Aadhaar is a 12 digit individual identification number issued by the Unique Identification Authority of India on behalf of the Government of India.

- Once the Aadhaar status is seen as generated, there is an option to print the Aadhaar from the web site. Click on the link [https://eaadhaar.uidai.gov.in/](https://eaadhaar.uidai.gov.in/) in the Resident Portal to open a window with all relevant details will have to be filled.
Chapter 7: The UIDAI Project

Exercises

1. What is UIDAI?
2. Explain importance of UIDAI.
3. What is e-Aadhaar?