RAJASTHAN E-GOVERNANCE IT & ITES POLICY 2015

Government of Rajasthan
Department of Information Technology &
Communication

RAJASTHAN E-GOVERNANCE IT & ITES POLICY 2015

October, 2015

INDEX

Definitions

1. “IT Sector” means manufacturing of hardware and software for Information Technology other than ESDM, and shall include development of IT software, IT services, IT enabled services, IT infrastructure, IT training institutions and robotics centre.
2. “IT Industries” include IT hardware & software industries. IT software industries include IT software, IT services, IT enabled services, IT infrastructure and IT training institutions. The “IT Industry” shall cover development, production and services related to IT products. Here IT includes IT & Telecommunications.
    a. “IT Software” is defined as any representation of instructions, data, sound or image, including source code and object code recorded in a machine readable form, and capable of being manipulated for providing interconnectivity to a user, by means of an automatic data processing machine falling under heading “IT Products”, but does not include “non-IT products”.
    b. “IT Products” are defined as computer, digital-data communication and digital-data broadcasting products as notified by the Ministry of Finance, Government of India or Central Board of Excise & Customs.
    c. “IT Service” is defined as any IT-based service which results from the use of any IT system for realizing value addition.
    d. “IT Enabled Service” is defined as any product or service that is provided or delivered using the resources of Information and Communication Technology.
    e. “IT Training Institution” means an institution imparting training in the field of IT, IT Enabled Service and IT Services and having an accreditation / affiliation from NIELIT (GOI) or any University established by Law in India or any Institution which has a Deemed University status as per the UGC Act.
    f. “IT Infrastructure” means the physical infrastructure built by a firm or a builder and sold / leased or transferred on lease-cum-sale to an IT industry for its use or the infrastructure built by an IT industry for its own use.
    g. “Telecommunications” means telecommunications companies including Basic Telecom Service Providers, VSAT, Cellular (Mobile) companies, Telecom

Infrastructure Companies, LAN, ISPs and any other value added services licensed by Ministry of Communications & IT, Government of India.

3. "Electronic System Design Manufacturing (ESDM)" means electronic hardware design and manufacturing (which shall include embedded software) for information technology, telecommunications, defense, medical, industrial automotive, robotics, consumer product, applications and components, part and accessories required for the aforesaid product and applications;
   a. "Robotics Enterprise" means an industrial undertaking or a business concern or any other establishment, by whatever name called, engaged in manufacturing, in any manner, or engaged in providing or rendering of service or services pertaining to robots, i.e. an automatically controlled, reprogrammable, multipurpose manipulator programmable in three or more axes;
4. "Backward Area" means an area as the Government may so notify by an order;
5. "CST" means tax payable under the Central Sales Tax Act, 1956 to the Government of Rajasthan;
6. "Commencement of Commercial Production/Operation" means:
   a. For a new enterprise, the date on which the enterprise issues:
      - the first sale bill of the goods manufactured related to the investment made under this Policy; or
      - the first bill of commercial transaction related to the investment made under this Policy; or
      - the first receipt of deposit of fee/charges etc. for providing any service with respect to facilities set up related to investment under this Policy; or

      Provided that investment made in development of an industrial park, it shall mean the date of handing over of possession to the first unit in the park.
   b. For an existing enterprise making investment for expansion, the date on which the enterprise issues:
      - the first sale bill of the goods manufactured after completion of expansion; or
      - the first bill of commercial transaction after completion of expansion; or
      - the first receipt of deposit of fee/charges etc. for providing any service with respect to facilities set up after completion of expansion:

      Provided that investment made in development of an industrial park, it shall mean

the date of handing over of possession to the first unit in the park.

   c. For revival of sick industrial enterprise, the date on which the enterprise issues the first sale bill of the goods manufactured after its revival;
7. "Conversion Charges" means the conversion charges payable to Government for change in land use and shall include any part of such charges payable to local bodies;
8. "Electricity Duty" means the duty payable under the Rajasthan Electricity (Duty) Act, 1962;
9. "Eligible Units": New units will be eligible for availing of incentives under this Policy. Existing units carrying out expansion/ diversification during the operative period of this Policy will be eligible for one-time incentives.
10. "Employment by an enterprise" means to employ any person, other than the directors, promoters, owners and partners, for wages or salary to do any manual, unskilled, skilled, technical or operational work, in or in connection with the work of an enterprise and who works either in the premises of the enterprise or engaged in Rajasthan outside the premises of enterprise and gets his/her wages or salary either directly from the enterprise or whose wages or salary is reimbursed by the enterprise;
11. "Enterprise" means an industrial undertaking or a business concern or any other establishment, by whatever name called, engaged in manufacture of goods, in any manner, or engaged in providing or rendering of service or services, as may be specified by an order by the State Government;
12. "Existing Enterprise" means a manufacturing or service enterprise that is engaged in commercial production or operation during the operative period of the Scheme;
13. "Existing Unit" means a manufacturing/service unit which is active with minimum 20 direct employees at the time of implementing expansion.
14. "Expansion" means creation of additional capacity for production of goods or operational capacity for service in same line of production/operation or through a new product line or new line of services by an existing enterprise provided that in case of expansion at existing site, additional investment is more than 25% of its existing investment on the date of initiating expansion at that site;
15. "Investment" or "Eligible Fixed Capital Investment (EFCI)" means investment made by an enterprise in fixed assets, in the following, up to the date of commencement of commercial production:

a. price paid for the land;
b. cost of new factory sheds and other new industrial buildings;
c. price paid for new plant and machinery or equipment;
d. other investment made in new fixed assets essential for production of the unit as approved by the Screening Committee; and
e. technical know-how fees or drawing fee paid in lump-sum to foreign collaborators or foreign suppliers or paid to laboratories recognized by the State Government or the Government of India;
f. However investment made in land in excess of 30% of the total investment/EFCI made and expenditure in purchase of existing factory sheds, industrial buildings and old plant and machinery by the Enterprise shall not be included in investment/EFCI;

16. "Land Tax" means the tax payable under chapter VII of the Rajasthan Finance Act, 2006;
17. "Large Enterprise" means a manufacturing enterprise other than Micro, Small and Medium Enterprises;
18. "Manufacturing Enterprise" means an enterprise employing plant and machinery in processing of goods which brings into existence a commercially different and distinct commodity and shall include an enterprise in the production of Commercial off-the-shelf software, but shall not include such processing as may be specified by the State Government by an order;
19. "Micro, Small or Medium Enterprise (MSME)" means a manufacturing enterprise notified as such under the Micro, Small and Medium Enterprises Development Act, 2006;
20. "Most Backward Area" means a block, which is more backward than backward area and is notified as such by the Government in the Finance Department, by an order;
21. "New Unit" means a new manufacturing or service enterprise set up by making investment within the meaning of clause 14 and includes a new unit set up by an existing enterprise at a site other than the existing site for manufacturing products or providing services which are different from those being manufactured or provided by it in the State, by making investment within the meaning of clause 14 and having separately identifiable books of accounts and depositing the taxes and duties leviable

under any State Act including Provident Fund separately;

22. "Person with disability (PwD)" means a person suffering from not less than forty per cent of any of the following disabilities:
    a. blindness;
    b. low vision;
    c. leprosy-cured;
    d. hearing impairment;
    e. locomotor disability;
    f. mental retardation;
    g. mental illness

    as certified by a Medical Authority i.e. any hospital or institution specified for this purpose by the Government of Rajasthan under the Persons with Disabilities (Equal Opportunities, Protection of Rights and Full Participation) Act, 1995;
23. "Revival of a Sick Industrial Enterprise" means, in case the sick industrial enterprise was lying closed due to sickness, re-commencement of commercial production, and in case of a running sick industrial enterprise, enhancement of production level due to infusion of fresh funds for change in production process/technology/product line, subject to condition that the enterprise provides employment to the extent of 50% in the first two years and 100% within five years from the date of commencement of commercial production of the maximum employment attained in any month of the 3 preceding years from the date of its declaration as a sick industrial enterprise;
24. "Service Enterprise" means an enterprise engaged in providing or rendering of services including custom made software development and related services, as the Government in the Finance Department may notify by an order;
25. "Sick Industrial Enterprise"means:
    a. A manufacturing enterprise which has been declared sick before the commencement or during the operative period of this Policy by the competent authority under the provisions the Sick Industrial Companies (Special Provision) Act, 1985; or
    b. A manufacturing enterprise, which has been taken over before the commencement or during the operative period of this Policy and sold during the operative period of the Scheme to a new management by RIICO/RFC/Central

Financial Institutions/Banks;

26. "Sick Industrial Enterprise" means:
    a. A manufacturing enterprise which has been declared sick before the commencement or during the operative period of this Policy by the competent authority under the provisions the Sick Industrial Companies (Special Provision) Act, 1985; or
    b. A manufacturing enterprise, which has been taken over before the commencement or during the operative period of this Policy and sold during the operative period of the Policy to a new management by RIICO/RFC/Central Financial Institutions/Banks;
27. "Stamp Duty" means the duty defined as stamp duty payable under the Rajasthan Stamp Act, 1998;
28. "State Empowered Committee (SEC)" means the State Empowered Committee constituted under Section 3 of the Rajasthan Enterprises Single Window Enabling and Clearance Act, 2011;
29. "Women/Schedule Caste (SC)/Schedule Tribe (ST)/Person with disability (PwD) enterprise" means an enterprise other than a Company constituted under the Companies Act, 1956 and other association of persons by whatsoever name it may be called, having:
    a. Women/Schedule Caste (SC)/Schedule Tribe (ST)/Person with disability (PwD) as proprietor, in case of proprietorship enterprise; or
    b. majority of partners who are Women/Schedule Caste (SC)/Schedule Tribe (ST)/Person with disability (PwD) and such partners are working partner(s) having more than 50% investment in the capital of the enterprise, in case of partnership including limited liability partnerships;
30. "VAT" means the tax payable under the Rajasthan Value Added Tax Act, 2003;
31. "Year" means financial year (From 1st April to 31st March) and quarter means the period of three months ending on 30th June, 30th September, 31st December and 31st March;

SECTION 1
Stratum of Digital Rajasthan

1.1 Preamble

e-Governance in Rajasthan has steadily evolved from computerization of Government departments to fragmented initiatives aimed at speeding up e-Governance implementation across the various arms of the Government at the State and local levels. These fragmented initiatives are being unified into a common vision and strategy under the Rajasthan e-Governance Framework leveraging the Rajasthan e-Governance Architecture.

Rajasthan takes a holistic view of e-Governance initiatives across the State and departments, integrating them into a collective vision and a shared cause. Around this idea, a magnanimous State-wide infrastructure reaching down to the remotest of villages is evolving, and large-scale e-Governance initiatives are taking place to enable easy, reliable access of people to the Government the e-Way.

Over the last few decades, evolutions in the Information Technology & Electronics (ITE) arena have emerged as the most significant enablers for improving efficiency & effectiveness of the Government & non-government organisations. Rajasthan recognizes the enormous potential of Electronics and Information technology and has made significant efforts to ensure that the benefits of these sectors percolate to its citizens.

Rajasthan's multicultural population of 6.86 crore lives and works on a land area of 342239 square kilometres, and has learned to combine skills and diligence with education and technology to sustain the momentum of economic growth. There is a recognition that information technology is needed to leverage Rajasthan's intellectual capital for the State to be the leader and benchmark for e-Governance. A concerted effort to harness computer power began in the early 1980s, and in a manner that has become a state formula, the Government has taken the leadership reins of the race.

e-Governance is seen as a key element of the Rajasthan's governance and administrative reform agenda. The Rajasthan e-Governance Framework and Architecture has the potential to enable huge savings in costs through the sharing of core and support

infrastructure, enabling interoperability through standards, and of presenting a seamless view of Government to citizens. The ultimate objective is to bring public services closer to citizens.

Rajasthan emphasises that creating digital opportunities in the 21st century is not something that happens after addressing "core" development challenges, but it is rather a key component of addressing those challenges. There are three key challenges in stepping up e-Governance: investments in and access to ICTs, capacity building to utilize e-Governance services, and promoting people's participation in e-democracy. It is hoped that improved access to information and services will provide economic and social development opportunities, facilitate participation and communication in policy and decision-making processes, and promote the empowerment of the marginalised groups.

In its continuing endeavour of development, the Rajasthan e-Governance, IT & ITES Policy 2015 envisages promoting citizen access to ICTs for encouraging their participation in e-Governance. The Policy is for the people, by the people. Though the 33 districts of Rajasthan are at various stages of development, the Policy attempts to highlight the possibilities for other districts that are similar to capital in levels of development. To promote the IT / ITES Industry in the city, this Policy attempts to develop a more modern and vibrant ecosystem for Electronics and IT industry to support electronic governance initiatives of the Government of India and attract investment and talent to such industries in Rajasthan. Key focus areas of the policy include pioneering e-Governance initiatives, research & development in Electronic System Design and manufacturing, support of the Micro Small & Medium Enterprises and promotion of entrepreneurship that harnesses the huge talent pool of the people of Rajasthan, and ensuring inclusive growth – for one and for all.

1.2 Rajasthan e-Governance & IT Mandate

A. Vision

To achieve good governance and facilitate inclusive growth, harnessing ICT and evolving e-Governance with improvement in delivery of services, bridging the digital divide and evolving Digital Rajasthan.

B. Mission

a) Establishing complete participatory & transparent open Governance and Citizen Centric IT and e-Governance for the residents of Rajasthan

b) Branding Rajasthan on the IT Landscape
   i. Establishing 7 Smart Cities in Rajasthan by 2020
   ii. Positioning Rajasthan as Best IT Investment Destination
   iii. Positioning and Branding Jaipur as IT, ITeS and R&D Hub in North and West India

c) Improvement in the environment for IT Industry in Rajasthan.

C. Objectives

a) Till 2025:
   i. Achievement of up to 500,000 direct employable professionals in the ICT sector vide implementation of ICT/ESDM initiatives in Rajasthan with establishment of Rajasthan Skills Registry.
   ii. Development of at least 2,000 technology startups in the State and prioritization of IT/ITeS/ESDM sector under Rajasthan Venture Capital Fund with specific capital for development of IT/ITeS/ESDM startups in Rajasthan.
   iii. Increase in the current investment in IT/ITeS sector by 10 times.
   iv. Increase in the IT turnover to INR 50,000 crore.
   v. Increase in IT exports from the State to INR 5000 crore.
   vi. Making two individuals (at least one female) in every household e-literate so as to bridge the digital divide.

b) Improvement in delivery of public services by leveraging e-Governance and m-Governance to achieve Efficiency, Effectiveness, Economy, Transparency, Accountability and Reliability in service delivery across all departments and functions and Re-engineer the

Objectives

Till 2025:

- **Make two individuals (at least one female) in every household e-literate**
- **Achieve up to 5,00,000 direct employable professionals in the ICT sector**
- **Develop at least 2,000 technology startups**
- **Prioritize IT/ITeS/ESDM sector**
- **Increase in the current investment in IT/ITeS sector, Increase IT turnover to INR 50,000 crore. and Increase in IT exports from the State to INR 5000 crore.**

Government business practices and rules to ensure hassle-free service delivery.

c) Ensuring requisite connectivity to all Government offices up to Panchayat level by 2016.

d) Creating centralized, integrated and unified state datasets to ensure uniformity, de-duplication and updating.

e) Providing secure e-Space for personal/official storage with facility for authentication and workflow to residents and organizations, private or public, in Rajasthan.

f) Rise in awareness among the school and college children and society as a whole regarding environmentally sound e-Waste management and take steps for its proper disposal.

g) Implementation of a uniform website policy for Rajasthan Government with emphasis on user-friendliness of the interface for all inclusive percolation of the benefits of IT.

h) Promotion of Robotics and Open Source Technology for IT initiatives in Rajasthan.

Objectives

- **Establishing Smart Cities**
- **Automated Service Delivery with automated one-time verification of Government documents**
- **Connectivity up to Panchayat level by 2016**
- **Centralized, integrated and unified State Datasets**
- **Promotion of Robotics**
- **Promotion of Open Source Technology**

SECTION 2
e-Governance for All

2.1 Service Delivery – e-Governance and m-Governance

A. Enabling actions shall be taken for implementation of existing and future e-Governance and m-Governance projects in the State with emphasis on Service Delivery, Right to Information and Grievance Redressal.

B. e-Enablement of all public services shall be carried out, which would include e-Submission of forms, electronic workflows, e-Payments, Use of DSC, online/SMS-based status tracking and final delivery of services through e-means. It would also include (wherever required) cross-sharing of data amongst various departments/Govt. agencies, and e-Authentication.

C. Uniform and Unified Datasets, collated centrally as a Hub shall be developed to take care of issues like duplication, isolation and obsolescence. In complete adherence to the State e-Governance Framework, such Datasets shall follow a common structure, shall be centrally located, controlled and managed, and shall provide complete flexibility of expansion and integration using state-of-the-art technologies.

D. Affidavits and Notary Attestation shall be completely removed and Datasets shall be used instead of documents for service delivery.

E. Individual, Family, Governmental and Organisational secure e-Space shall be provided to residents and organisationsto enable them to secure their digital dialog and

- **Easy access and delivery of all Government services:**
  - **Automated Unified Service Delivery and benefits transfer using e-Mitra and Bhamashah**
  - **Unrestricted and seamless means of service delivery – Web Portals, Mobile, e-Mitra Kiosks**
  - **Automated electronic verifications and secure storage – Raj eVault**
- **Next Generation IT Infrastructure:**
  - **Connectivity till village level (RajNET)**
  - **Complete readiness for mobile governance**

to allow safe document storage, sharing, e-Sign and approval protocol to avoid providing attestation of duplicate documents, enabling service delivery through all Government departments centrally in a paperless fashion.

F. One Person One e-Identity shall be achieved with unique online profile for each citizen under a common framework.

G. For delivering e-Services to citizens, Government will promote the use of upcoming technologies like NFC, cloud computing and social media. Further, multiple channels like mobile phones, tablets, call centres, TV, etc. will be used for such delivery.

H. Efforts would be undertaken to provide all government services through mobile devices for 'on-the-move' service delivery. Endeavour will be to provide services 'Anywhere, Anytime, Any network, Any device'.

I. Self-service kiosks shall be installed across the State.

J. An integrated platform for reality check leveraging iFacts shall be used by the government to ensure end-to-end grievance redressal.

K. An endeavour would be made to analyse the behaviour of the citizens in usage of Government portals so as to constantly improve these portals and make them more user friendly.

L. Knowledge resources / Digital Library will be set-up that will maintain a repository of documents for use by general public and Govt. authorities. This would include official gazette notifications, acts, rules, regulations, circulars, policies and scheme documents for electronic access in a time-bound manner.

2.2 Office Automation

A. Government shall notify the acceptance of correspondence through emails received from the public. Further, use of official email ID would be mandated by Government for all official communications, which, inter alia, includes (i) responding to such correspondence of citizens, and (ii) for intra- and inter-departmental communication within Government and communication with Govt. of India to make citizen-government interface more efficient and effective.

B. Complete office automation in an integrated fashion shall be carried out, with end-to-end automated office processes and workflow automation, and shall ensure all government departments integrated on a common platform.

C. Common Gateway for all citizen services with corresponding required information available to public leveraging eMitra Integrated Service Delivery Platform and Bhamashah.

D. Integrated GIS-based Decision Support System shall be implemented and commissioned with GIS Mapping and Layers for all respective departments, and Government shall mandate the use of only this GIS-based decision making system by all departments.

- **Automation of all Government offices**
  - **GIS-based Decision Support System with GIS Mapping (Rajdharaa)**
  - **Centralized Grievance Redressal (Rajasthan Sampark)**
  - **Centralized Monitoring and Accountability System (RAAS & iFacts)**
- **Unification of Government information — creation of Centralized Data Repository**
- **'Anywhere, Anytime, Any network, Any device' service delivery through mobile phones, tablets, call centres, TV, etc.**
- **One Person One e-Identity with unique online profile for each resident**
- **Creation of next generation IT Infrastructure**

2.3 IT Infrastructure

A. Creation of next generation IT Infrastructure and up-gradation of existing IT infrastructure shall be undertaken to bring it at par with the world class state-of-the-art infrastructure.

B. Further, development of IT infrastructure shall be undertaken to support the increasing requirements of Rajasthan including the rural areas to ensure that high speed internet connectivity reaches every citizen.

C. Extended State Data Centre to provide 'on-the-go' services through an integrated cloud-based mechanism to all the departments to minimize the overheads associated with managing the physical infrastructure and to ensure that all the components of IT infrastructure (Hardware, Software, Network, etc.) would be available as simple and configurable services.

D. Government shall endeavour to provide every state resident with high speed internet access (wired and wireless) for creation of smart city infrastructure This will be achieved, inter alia, through (i) making 7 Wi Fi cities in Rajasthan (ii) creation of fibre-ready urban homes.

E. Government shall encourage Green IT initiatives. Departments shall be disposing off their unusable, redundant and irreparable IT infrastructure as per the guidelines of e-Waste management. For this, guidelines on the obsolescence of IT hardware will be formulated.

F. Rajasthan Information Security Policy shall promote public trust in Government, with continual improvements to protect the State from cyber attacks and cyber-disruptions, thus enhancing preparedness, security and resilience.

SECTION 3
Bridging Human Capital Divide

3.1 Capacity and Skill Building

- **Making two individuals (at least one female) in every household e-Literate**
- **Facilitating partnership between educational institutes and industry**
- **Utilising Digital India and Digital Rajasthan campaign for mass literacy**
- **Creating Rajasthan Skills Repository with Data bank of youth who are IT literate**

A. Rajasthan e-Governance Centre of Excellence with a mandate of IT for Jobs and Employability Assurance, Rural ICT workforce development and IT Education Incubation Units shall be established, and shall become the central authority for Capacity and Skill Building in IT/ITeS/ESDM/R&D fields in Rajasthan. This CoE shall be:

a) Strengthening of IT & Personality Development Program/soft skills curriculum with significant weightage in overall performance/grades and spreading of awareness about job opportunities in IT.

b) Standardized IT/ ITeS/ BPO/ KPO/ ESDM/ ITES-BPO certification for job aspirants for the industry. The certification shall be granted by relevant authorities in Government in association with the private sector thus adding credibility to the IT professional skills, reducing time and cost of hiring for recruiters.

c) Facilitating training and development of IT skills as well as personality development program for teachers and encouraging them to use IT to enhance the effectiveness of teaching.

d) Encouraging introduction of IT Clubs for students & faculty.

e) Facilitating partnership between educational institutes and industry to provide courses/ training on emerging IT technologies.

f) Facilitating setting up of e-Learning centres, in rural/ slum areas for promotion of IT education along with soft skills development and spreading awareness about job opportunities in IT.

g) Transforming non-IT human resource to IT specialities taking advantage of Digital India and Digital Rajasthan campaign.

h) Strive towards digital economy and knowledge based society drawing upon the strength of Digital Rajasthan.

B. Possibility of introducing distance learning program/ vocational courses shall be explored in this respect. This would enable "anytime anywhere" learning.

C. Spreading awareness about job opportunities in IT and facilitating short-term job oriented certificate courses in various IT skills and Personality Development Program for unemployed educated youth shall be done.

D. Rajasthan Skills Repository with Data bank of students who are IT literate and suitable for deployment in the IT industry would be established, maintained and shared with the industry. This would enable the industry to have easy access to skilled manpower.

SECTION 4
Inclusive Industry Promotion

4.1 IT/ITeS Industry Development

A. Benefits to Manufacturing Enterprises

a) Investment up to Rs.5 crore

i. Investment subsidy of 30% of VAT and CST which have become due and have been deposited by the enterprise for seven years.

ii. Employment Generation Subsidy up to 20% of VAT and CST which have become due and have been deposited by the enterprise, for seven years.

b) Investment more than Rs.5 crore and up to Rs.25 crore

i. Investment subsidy of 60% of VAT and CST which have become due and have been deposited by the enterprise, for seven years.

ii. Employment Generation Subsidy up to 10% of VAT and CST which have become due and have been deposited by the enterprise, for seven years.

c) Investment more than Rs.25 crore

I. Investment subsidy of 70% of VAT and CST which have become due and have been deposited by the enterprise, for seven years.

ii. Employment Generation Subsidy up to 10% of VAT and CST which have become due and have been deposited by the enterprise, for seven years.

The total amount of subsidy as mentioned above shall not exceed 100% of EFCI.

- **VAT/CST Incentive – Investment & Employment Generation Subsidy**
  - **Up to 80% for Manufacturing**
  - **Up to 90% for Women, SC, ST, Persons with Disability**
  - **Up to 100% for Backward and Most Backward Areas**
  - **Up to 80% of VAT Reimbursement for Services Industry**
  - **Up to 50% exemption on Land Tax, Electricity Duty, Entry Tax**
  - **Up to 100% exemption on Stamp Duty**

d) Exemption from payment of 50% of Electricity Duty for seven years.
e) Exemption from payment of 50% of Land Tax for seven years.

B. Benefits to Service Enterprises

a) Reimbursement of 50% of amount of VAT paid on purchase of plant and machinery or equipment for a period up to seven years from date of issuance of the entitlement certificate, provided that for enterprises engaged in providing entertainment, the reimbursement shall be restricted to 25% of such amount of VAT paid;
b) Exemption from payment of 50% of Electricity Duty for seven years
c) Exemption from payment of 50% of Land Tax for seven years.

C. Special Provisions for Women, Scheduled Castes, Scheduled Tribes and Persons with Disability Enterprise

Eligible Women/Schedule Caste (SC)/Schedule Tribe (ST)/Person with disability (PwD) enterprises shall in addition to the benefits specified in other clauses, be eligible to avail the following additional benefits:

a) A manufacturing enterprise shall get additional Investment Subsidy to the extent of 10% of VAT and CST which have become due and have been deposited by the enterprise.
b) A service enterprise shall get additional 10% reimbursement of VAT paid on the plant and machinery or equipment for a period up to seven years from date of issuance of the entitlement certificate for this purpose.

D. Benefits to Enterprises in Backward and Most Backward Areas

a) An eligible enterprise, making investment in a backward area or a most backward area shall be granted the same benefits as would have been applicable if the enterprise was located elsewhere in the State but the period of benefit, except for interest subsidy, shall be extended to ten years.
Provided that the State Government may, on the recommendation of the State Empowered Committee (SEC), grant to a manufacturing enterprise and a service enterprise making an investment in a backward area, such benefits as mentioned in below mentioned clauses b and c respectively, which are applicable for investments in most backward areas, with a view to attract investment in the backward area.
b) A manufacturing enterprise, making investment in a most backward area shall, in addition to benefits under clause a above, get additional investment subsidy of 20% of the VAT and CST which have become due and have been deposited by the enterprise, for a period of seven years.
c) A service enterprise making investment in a backward area shall, in addition to benefits mentioned in other clauses of the Scheme, get additional 10% reimbursement of VAT paid and a service enterprise making investment in a most backward area shall, in addition to benefits mentioned in other clauses, get additional 20% reimbursement of VAT paid on the plant and machinery or equipment for a period up to seven years from the date of issuance of the entitlement certificate for this purpose.

Special Customized Packages as per RIPS 2014 and subsequent amendments/ addendums

E. Power to Grant Customized Package

a) Notwithstanding anything contained in the Scheme, the State Government, on the recommendation of State Empowered Committee (SEC), may grant a customized package under section 11 of the Rajasthan Enterprises Single Window Enabling and Clearance Act, 2011, to the manufacturing enterprises investing more than Rs.200 crore or providing employment to more than 400 persons.
b) Notwithstanding anything contained in the Scheme, the State Government may grant a customized package to the service enterprises investing more than Rs.200 crore or providing employment to more than 500 persons.

F. MSME Sector

Manufacturing enterprises in the MSME sector shall, in addition to benefits mentioned above, if applicable, be granted the following benefits:

a) For micro and small enterprises in rural areas, 75% exemption from payment of electricity duty in place of 50% exemption from payment of electricity duty, as provided in notification number F.12(99)FD/Tax/07-56 of 15.10.2009, as amended from time to time.

b) Reduced CST of 1%, against C Form, on sale of goods for a period of ten years, for micro and small enterprises as provided in notification number F.12(99)FD/Tax/07-66 of 14.02.2008 as amended from time to time;

c) 50% exemption from payment of Entry Tax on raw and processing materials and packaging materials excluding fuel as provided in notification number F.12(99)FD/Tax/07-65 of 14.02.2008 as amended from time to time; and

d) Reduced Stamp Duty of Rs.100 per document in case of loan agreements and deposit of title deed and lease contract and Rs.500 per document in case of simple mortgage with or without transfer of possession of property executed for taking loan for setting up of micro, small or medium enterprises or enhancing credit facilities or transfer of loan account from one bank to another by MSME as provided in notification number F.2 (97)FD/Tax/2010- 11 of 25.04.2011.

G. ESDM Sector

Enterprises making a minimum investment of Rs.25 lakh rupees in the ESDM sector shall, be granted the following benefits:

a) Investment Subsidy of 75% for first four years, 60% for next three years and 50% for the last three years, of VAT and CST which have become due and have been deposited by the enterprise, for ten years;

b) Employment Generation Subsidy up to 10% of VAT and CST which have become due and have been deposited by the enterprise, for ten years; and

c) 50% exemption from payment of Entry Tax on capital goods, for setting up of plant for new unit or for expansion of existing enterprise or for revival of sick industrial enterprise, brought into the local areas before the date of commencement of commercial production/operation.

H. Robotics Centre

The State shall promote establishment of Robotics Centres acting for the future of

robotics by casting the vision, and supporting the technology of robotics through Robotics enterprise promotion in Rajasthan. On investments of Rs.50 crore or more for establishment of such centres, Interest Subsidy of 5% on term loan taken from State Financial Institution/Finance Institution/banks recognized by RBI subject to a maximum of Rs.10 lakh per year for a period up to 5 years or up to the period of repayment of loan, whichever is earlier, from the date of commencement of the centre shall be provided.

Interest subvention on investment upto Rs.50 crore for Robotics

I. Benefits for Internet Connectivity

- Subsidy on Bandwidth for Connectivity (for BPOs/KPOs)
  25% subsidy on Bandwidth for connectivity paid to Internet Service Provider (ISP), subject to maximum of Rs.5 lakh per annum, shall be available for a period of two years from the date of starting commercial production/operation. The subsidy amount will be determined on the basic benchmark prices to be declared by Government separately.
- Gateway and High Bandwidth Backbone
  The State Government shall encourage private sector to become ISPs in the districts and set up international gateways in the State. The State Government shall facilitate and promote the establishment of broadband digital network (both wired and wireless) in the State.

J. Rajasthan Venture Capital Fund/SME Tech Fund RVCF II

25% of Rajasthan Venture Capital Fund shall be en-marked for IT/ITeS Sector. SME Tech Fund RVCF II with a committed corpus of over Rs.155 crore, raised by RVCF shall support enterprises in the high tech/emerging sectors that are of value to the Indian Economy,

- **25% subsidy on Internet Bandwidth**
- **Venture Capital**
  - **25% of Rajasthan Venture Capital Fund en-marked for IT/ITeS Sector**
  - **RVCF SME Tech Fund II for IT/ITeS Sector**
- **Exemption from Zoning Regulations and Land Conversion to IT Parks/IT Campuses, IT Industry**

commercially viable in terms of profitability and exhibit substantial future growth potential.

IT/ITeS enterprises shall be eligible for support from this fund.

K. Exemption from Zoning Regulations and Land Conversion

IT Parks/IT Campuses notified by the Department of Industries/Department of IT&C and IT industry, i.e., IT/ITES Units/Companies shall be exempted from the Zoning Regulations and payment of conversion charges, subject to the provisions of State Acts and the following:

- a maximum area limit (to be notified separately)
- ensuring environmental safeguards

L. Stamp Duty and Registration Fee Exemption

a) Enterprises with investment up to Rs.5 crore shall be provided 50% exemption from payment of stamp duty on purchase or lease of land and construction or improvement on such land.

b) Enterprises with investment of Rs.5 crore and more shall be provided 100% exemption from payment of Stamp Duty on purchase or lease of land and construction or improvement on such land.

M. Interest Subsidy

Service Enterprises making investment more than Rs.25 lakh shall be provided 5% Interest subsidy on Term Loan taken from State Financial Institutions/ Financial Institutions/ Bank recognized by Reserve Bank of India for purchase of equipment required for rendering services related to IT/ITeS Sector, subject to a maximum of Rs.5 lakh per year for a period of 5 years or up to the period of repayment of loan, whichever is earlier, from the date of commencement of commercial operation.

The enterprises which are engaged in manufacturing and rendering of services both, in IT/ITeS Sector, shall have an option to opt for:

a. Investment Subsidy and Employment Generation Subsidy, or
b. Interest Subsidy

- **Upto 5% Interest Subsidy on term loans**
- **Reimbursement of Patent Filing Costs upto Rs.3 lakh per patent awarded per year**
- **30% Reimbursement of Quality Certification Costs upto Rs.5 lakh**

N. Patent Filing Costs

The Government of Rajasthan is keen to encourage the filing of patents by companies located within the State. The Government will, therefore, reimburse the cost of filing patents to companies having their headquarters in Rajasthan for successfully receiving patents. Reimbursement of such cost will be limited to a maximum of Rs.3 lakh per patent awarded per year.

O. Networking and Business Growth Support

- Business Networking
  Government shall promote and encourage participation in international events by the ICT industry in form of joint delegation.

P. Quality Certifications

The Government of Rajasthan will reimburse 30% of expenditure incurred for obtaining quality certifications for CMM Level 2 upwards. Reimbursement will be limited to a maximum of Rs.5 lakh. Similar reimbursement will be made to BS7799 for security and also for ITES Companies for achieving COPC and eSCM certifications. The IT/ITES units/companies/firms can claim this incentive only once. A company/firm can claim incentive for BS7799 or any one of CMM Level 2 upwards/COPC/ eSCM.

Q. Protection of IPR

There will be a legal mechanism to control piracy of information technology products. Intellectual Property Right (IPR) protection support will be given to all entrepreneurs developing software and animation. All online transactions would be secured by a fool-proof mechanism of digital signature and biometric-like

Outstanding Performance Awards in 4 categories with a grant of Rs1.5 lakh for each award

fingerprint and its recognition.

R. Outstanding Performance Awards

Registered IT/ITES units in the State will be considered for 'Outstanding Contribution Award' in form of grant each year in each category on the basis of objective criteria published by the Government.

Awards shall be given to the following categories:

- New Ventures – Most Promising Venture
- IT Enterprises – Best performing IT Company
- Innovation Leader – Enterprise that has displayed the maximum innovation in its products and services
- Startup Ventures

A total of 3 awards shall be given in each category, with a Grant of Rs.1.5 lakh for each award.

S. Incubation Units

The state shall be promoting sectorial incubation units for development of concerned sector, in partnership with industry and academia. IT/ITeS/ESDM/R&D Incubation Units in Sitapura EPIP Zone shall be promoted by the State.

T. Manpower Development Subsidy

Subsidy on Manpower development shall be provided in respect of Training/Technical up-gradation/Skill up gradation of local persons in a registered training organization/institution subject to a ceiling

Investment in fixed capital	Total Ceiling
Up to Rs.25 lakh	Rs.1.5 lakh
Rs.25 lakh to 50 lakh	Rs.3 lakh
Rs.50 lakh and above	Rs.5 lakh

Reimbursement on fixed capital up to Rs.5 lakh for Manpower Development

U. Auxiliary Support for Investors

All IT companies would be notified as 'Public Utility Service' providers under the Industrial Disputes Act, 1947.

All IT units, given the nature of their operations, will be granted permission to work on a 24x7 model.

4.2 General Incentives

General incentives available to the ICT industry, automatically are:

a) IT/ITES units are exempt from the purview of the Pollution Control Act, except in respect of power generation sets.

b) IT/ITES units/companies are exempt from the purview of statutory power cuts.

c) The regulatory regime of labour laws shall be simplified to suit the needs of IT & ITES companies. General permission shall be granted to all IT & ITES companies to have 24x7 operations/to run in three shifts.

d) Barriers pertaining to employment of women at night shall be removed, the companies will be instructed to offer employment to women with adequate security to them for working at night.

e) The IT & ITeS companies will be permitted to self-certify that they are maintaining the registers and forms as contemplated and prescribed under the following Acts:

i. The Payment of Wages Act, 1936
ii. The Minimum Wages Act, 1948
iii. The Workmen's Compensation Act, 1923
iv. The Contract Labour (Regulations and Abolition) Act, 1970
v. Employees State Insurance (Amendment) Act, 2010
vi. Bombay Shops and Establishment Act
vii. The Payment of Gratuity Act, 1972
viii. The Maternity Benefit Act, 1961
ix. Equal Remuneration Act, 1976
x. Water (Prevention and Control of Pollution) Act, 1974
xi. Employment Exchange Act, 1959
xii. The Factories Act, 1948
xiii. Employees' Provident Fund & Miscellaneous Provisions Act, 1952

f) IT/ITES units/companies and non-hazardous hardware manufacturing industry are declared as essential service.

SECTION 5
Green IT

5.1 Condemnation and Disposal of IT Equipment

A. Applicability

a) All Departments/Companies/Corporations/Institutions/Organizations/Bodies on whom this Policy is applicable must ensure that there are proper procedures in place for the condemnation and disposal of IT equipment that is unserviceable or is no longer required. This Policy shall be applicable to the following departments and bodies:

i. All Government Departments under the aegis of Government of Rajasthan
ii. All Companies/Corporations/Autonomous Bodies/Local Bodies under the aegis of Government of Rajasthan
iii. All PSUs under the aegis of Government of Rajasthan

B. Definition of IT Equipment

a) Hardware

By its own nature IT equipment is constantly evolving and this can therefore become a very broad category making it impossible to list every single item or group of items within this policy document; however a non-exhaustive list of IT and related equipment to be considered for this purpose is associated.

b) Software

Software can be summarized as follows:

i. Desktop Software: all applications and related data loaded onto a desktop or laptop computer.
ii. Server Software: all applications and related data loaded onto a local or networked server.
iii. Hosted Solution: all applications and related data (owned by GoR) hosted on/off site.

C. Useful life of various items and replacement

Depending upon the nature, usage, maintenance cost, obsolescence in terms of technology, up-gradation of technology, etc., the related items are classified in following categories for the purpose of disposal of these items. The detailed non-exhaustive list of category-wise items is available in section 5.2:

Category	Nature	Suggestive Items	Useful/Productive Life
I	Immediate obsolescence / use-and-throw products	Printing Consumables (Non-refillable Ink Toners), CDs, DVDs, Digital Audio Tapes (DAT), UPS Batteries	As per usage. No residual value determined. However, proper inventories of purchase, issue and final use/disposal, etc. would be maintained in order to keep an accounting system.
II	Low life/ Fast obsolescence products	Mobile Phones	Two years
		Laptops, Pen Drive, External Hard Disk Drive (HDD), etc.	Three years in case of Laptops, Pen Drive, HDD, etc. for replacement. Residual values determined separately.
III	Medium obsolescence / Medium life products	Desktops, Printers, Multi-functional Devices (MFDs), Scanners, Multi-media Projectors, UPS Systems,	Five years for replacement.
IV	Slow obsolescence/ long life products	Fax, EPABX, Electronic items such as cameras, TVs, DVD Players, Public Address Systems, Electronic Calorie Meter, etc.	Seven years
V	Software	Software like MS Office, Oracle, MS-SQL, MS-Windows, Antivirus, etc.	Please refer to the explanation given below.

Note: The above mentioned items can be used beyond the mentioned/specified life till such time these items continue to serve the purpose.

a) Use-and-throw products: These products have no fixed life and can be used till these are consumed or are under replacement warranty (like SMF batteries are covered under 1 year replacement warranty from the manufacturer). However, the user departments must maintain proper inventory of purchase, issue and disposal thereof so as to ensure prudent official use of these items.

b) Low life products: The general useful/productive life in the case of products/items in this category would be two years in the case of a Mobile Phone Instrument and three years in the case of laptops and other items mentioned therein for replacement purposes. However, one may use the same for longer period so long as the item/equipment serves the purpose.

c) Medium life products: The useful/productive life of products in this category is fixed at 5 years even though the products can be continued to be used for longer period in an organisation/department, being a multiple level of usage in terms of level of works to be done like Software development/testing, Data Processing, Information searching, Word processing, etc. Accordingly, the life of these products is fixed as five years for replacement purposes. However, one can use the equipment for longer period so long as it fulfills the user requirements.

d) Long life products: It has been observed that these products can be used for more than 5 years due to comparative stability in specifications/services. Accordingly, the replacement life of these products is fixed as 7 years. However, one can use the same for longer periods so long as these products serve the user requirements.

e) Software: Purchase of software can be booked as a one-time office expenditure. The old software can be upgraded into latest version by taking the benefit of old purchase in case scheme is available from the developer/principal company. In the alternative, latest software can be purchased and in that case the residual value of the old software can be treated as NIL. The old software can be donated to the State/Central recognised Service/Education Organisations.

D. Grounds for condemnation

For all condemnation cases, the concerned department shall form a committee comprising minimum 3 members, one of which shall be from the finance/accounts department and one member shall be a representative of DoIT&C in the department. If

in case there is no member of DoIT&C in the concerned office, the matter shall first be escalated to the HO of the concerned department and if not resolved, then to the DoIT&C.

The ICT Products/Equipment can be condemned on following grounds:

a) Technically obsolete
   i. Completed the life span as mentioned in Clause 4 and 5 and currently not in working condition.
   ii. Technology outdated affecting performance and output that is expected out of it.
   iii. Package Software can only be condemned by declaring it as technically obsolete when no more updates or support are available from OEM.

b) Beyond Economical Repairs
   ICT Products/Equipment can be declared BER when these Products/Equipment cannot be upgraded or maintained economically/warrant extensive repairs and replacement of sub-assemblies/accessories and the combined cost of which exceeds certain percentage (50%) of the current cost of an equivalent system. The same can be ascertained from the vendor who is giving AMC support.

c) Non-repairable
   ICT Products/Equipment can be condemned due to non-availability of spare-parts.

d) Physically damaged
   ICT Products/Equipment that have been damaged beyond repair due to fire or any other reason beyond human control can be condemned as Physically Damaged.

E. Disposal/alternate Use

a) The primary mechanism of alternate use, which must be considered in cases where the said item(s) are still in usable condition, should be to transfer the item(s) to Government School(s) of the districts in which the said office is located.

b) For this purpose, if the said item(s) are found usable by the DoIT&C representative in the department, a committee with DEO/BEO should be constituted to decide where the items can be sent for optimum usage.

c) Only if the possibility of usage by Government schools is found negligible, should the process of disposal be initiated by the department/office.

d) The mode of Condemnation may be done either by Buyback or Disposal, as decided by the committee formed for condemnation by the concerned department.

e) Buyback

If the committee decides to choose Buyback mode of Condemnation, the proposal for purchasing new ICT Products/Equipment under buyback mode will be sent by the concerned Department to DoIT&C for obtaining NOC. The Buyback rates for specific hardware as finalized in the ongoing Rate Contract shall be applicable. If the Buyback rates are not specified in the Rate Contract then the committee will decide the Buyback rates based on their assessment, after comparing similar Rate Contract in the past and in consultation with the Vendor.

f) Disposal

If the committee decides to choose disposal mode of Condemnation, the concerned Department can dispose it through Tender, Auction or Scrap depending on assessed residual value of the ICT Products/Equipment and as per the procedure laid down in this Policy document.

i. For the Products/Equipment with residual value above Rs.2 Lakh, the Department can dispose it through Advertised Tender or Public Auction.

ii. For Products/Equipment with residual value less than Rs.2 Lakh, the mode of disposal will be determined by Department's Competent Authority, keeping in view the necessity to avoid accumulation of such Products/Equipment and consequential blockage of space and also the deterioration in value of Products/Equipment to be disposed of.

F. Process of Disposal through Advertised Tender

The broad steps to be adopted for this purpose are as follows:

a) Preparation of bidding documents
b) Invitation of tender for the condemned ICT Products/Equipment to be sold
c) Opening of bids
d) Analysis and evaluation of bids received
e) Selection of highest responsive bidder
f) Collection of sale value from the selected bidder

g) Issue of sale release order to the selected bidder
h) Release of the condemned ICT Products/Equipment that were sold to the selected bidder
i) Return of bid security to the unsuccessful bidders

The important aspects to be kept in view while disposing the condemned ICT Products/Equipment through advertised tender are as under:

a) The basic principle for sale of condemned ICT Products/Equipment through advertised tender is ensuring transparency, competition, fairness and elimination of discretion. Wide publicity should be ensured of the sale plan and the Condemned ICT Products/Equipment to be sold. All the required terms and conditions of sale are to be incorporated in the bidding document comprehensively in plain and simple language. Applicability of taxes, as relevant, should be clearly stated in the document.

b) The bidding document should also indicate the location and present condition of the condemned ICT Products/Equipment to be sold so that the bidders can inspect the condemned ICT Products/Equipment before bidding.

c) The bidders should be asked to furnish bid security along with their bids. The amount of bid security should ordinarily be ten per cent of the assessed or reserved price of the condemned ICT Products/Equipment. The exact bid security amount should be indicated in the bidding document.

d) The bid of the highest acceptable responsive bidder should normally be accepted. There should normally be no post tender negotiations. If at all negotiations are warranted under exceptional circumstances, then it can be with HT (Highest Tenderer) if required.

e) In case the total quantity to be disposed of cannot be taken up by the highest acceptable bidder, the remaining quantity may be offered to the next higher bidder(s) at the price offered by the highest acceptable bidder.

f) Full payment, i.e. the residual amount after adjusting the bid security should be obtained from the successful bidder before releasing the condemned ICT Products/Equipment.

g) In case the selected bidder does not show interest in lifting the sold condemned ICT Products/Equipment, the bid security should be forfeited and

other actions initiated including re-sale of the condemned ICT Products/Equipment in question at the risk and cost of the defaulter, after obtaining legal advice.

G. Process of Disposal through Auction

a) The Department may undertake auction of condemned ICT Products/Equipment to be disposed of either directly or through approved auctioneers.

b) The basic principles to be followed here are similar to those applicable for disposal through advertised tender so as to ensure transparency, competition, fairness and elimination of discretion. The auction plan including details of the condemned ICT Products/Equipment to be auctioned and their location, applicable terms and conditions of the sale, etc. should be given wide publicity.

c) While starting the auction process, the condition and location of the condemned ICT Products/Equipment to be auctioned, applicable terms and conditions of sale etc., should be announced again for the benefit of the assembled bidders.

d) During the auction process, acceptance or rejection of a bid should be announced immediately. If a bid is accepted, earnest money (not less than twenty-five percent of the bid value) should immediately be taken on the spot from the successful bidder either in cash or in the form of Deposit-at-Call-Receipt (DACR), drawn in favour of the Department selling the condemned ICT Products/Equipment.

e) The condemned ICT Products/Equipment should be handed over to the successful bidder only after receiving the balance payment.

f) The composition of the auction team will be decided by the competent authority. The team should however include an Officer of the Internal Finance Wing of the Department.

g) A sale account should be prepared for goods disposed of, duly signed by the officials who supervised the sale or auction.

H. Process of Disposal at Scrap Value or by Other Modes

a) If the Department is unable to sell condemned ICT Products/Equipment in spite of its attempts through auction and advertised tender, it may dispose-off the same at its scrap value with the approval of the competent authority in consultation with

Finance division.

b) In case the Department is unable to sell condemned ICT Products/Equipment even at its scrap value, it may adopt any other mode of disposal including destruction of the Products/Equipment in an eco-friendly manner so as to avoid any health hazard and/or environmental pollution and also the possibility of misuse of such Products/Equipment.

c) All rules, regulations and norms of e-Waste Management, Energy Efficiency and bio-friendly disposal of all electronic waste containing substances like Lead, Cadmium, Mercury, PVC that have the potential to cause harm to human health and environment must be followed by the departments.

I. Responsibility of Department

a) Each unit of department will prepare equipment condemnation note which should be individually numbered having equipment description, including the make, model, serial number, asset register number, purchase date, purchase price, reason for condemnation and additional information, if any.

b) Department will constitute a condemnation committee which will review all condemnation notes and decide about the condemnation of equipment as per guidelines given above. The committee should have at least one member from accounts/finance background and also the representative of DoIT&C in the department as a member.

c) All procedure and rules made under relevant Rules of the Government on maintenance of records for condemnation of non-consumables items will be made in these cases.

d) The condemnation report so prepared by the department based on these guidelines will be sent to the headquarters of concerned department for approval by the nodal officer. The condemnation will be done only after approval is obtained from the headquarters of the said department. To avoid piece-meal approach, all cases of a department may be processed once a year in May-June.

5.2 LIST OF ICT EQUIPMENT

Category I

- CD ROM/DVD/Compact Disk
- Floppy Disk
- Tapes DAT/DLT
- Ribbons
- Toners – non refillable
- Ink jet cartridges
- Inks for output devices
- Any type of Cell/Batteries beyond repair

Category II

- Laptop Computers
- Note book Computers
- Palm top Computers/PDA
- iOS/Android/ Windows based mobile & smartphones, iPad/ Tablets
- Hard Disk Drives / Hard Drives
- RAID Devices & their Controllers
- Floppy Disk Drives
- CD ROM drives
- Tape Drives – DLT Drives / DAT
- Optical Disk Drives
- Other Digital Storage Devices, Pen Drive, Memory Card
- Key Board
- Monitor
- Mouse
- Multi-Media Kits
- Access Card
- Electronics Purse
- Electronics Wallet
- Universal Pre-payment card
- Smart card etc.

Category III

- Desktop
- Personal Computer
- Servers
- Work-station
- Nods
- Terminals
- Network PC
- Network interface card (NIC)
- Adaptor-ethernet/PCI/EISA/combo/PCMCIA
- SIMMs-Memory
- DIMMs-Memory
- Central Processing Unit (CPU)
- Controller-SCSI/Array
- Processors-Processor/Processor Power Module/Upgrade
- Dot-matrix printers
- Laser jet printers
- Ink jet printers
- Desk jet printers
- LED printers
- Line printers
- Plotters
- Pass book Printers
- Hubs
- Routers
- Switches
- Concentrators
- Trans-receivers
- Switch Mode Power Supplies
- Uninterrupted Power Supplies

Category IV

- Telephones
- Videophones
- Facsimile Machines/Fax cards
- Tele-Printers/Telex machines
- PABX/EPABX/RAX/MAX –Telephone exchange
- Multi plexers/Muxes
- Modems
- Telephone Answering Machines
- Tele-Communication Switching Apparatus
- Antenna & Mast
- Wireless Datacom Equipment
- VSATs
- Video Conferencing Equipment
- Including Set Top Boxes for both Video and Digital Signalling
- Fibre Cable
- Copper Cable
- Cables
- Connectors, Terminal Blocks
- Jack Panels, Patch Cord
- Mounting Cord, Patch Panels
- Back Boards, Wiring Blocks
- Surface Mount Boxes
- Printed circuit Board Assembly/populated PCB
- Printed Circuit Board/PCB
- Transistors
- Integrated Circuits/ICS
- Diodes/Thyristor/LED
- Registers
- Capacitors
- Switches (On/Off, Push- button, Rocker, etc.)
- Plugs/Sockets/Relays

- Magnetic Heads, Print Heads
- Connectors
- Microphones/Speakers

Category V

- Application Software
- Operating System

SECTION 6
Digitally Secure Rajasthan

6.1 Information Security Policy

A. Foundation of Information Security

The State of Rajasthan recognises its dependence on information systems for effective operations of its e-Governance Initiatives. It is, therefore, essential that this information infrastructure is secure from destruction, corruption, unauthorized access, and breach of confidentiality, however accidental or deliberate.

Information Security requirements are of utmost importance for the State. Successful internal co-operation requires that a common security concept prevails in the GoR.

The objective is to define standards to ensure that information is secure at all times, in turn creating a foundation upon which sound internal controls within the computerized environment can be exercised. This is applicable to all officers and officials associated with Rajasthan Government/Boards/Corporation/PSUs/Third Parties.

It is vital that we continue our efforts with security and risk management so as to equip ourselves to meet the challenges of service running catering to the citizens of the State and give each User Department the means to fulfil its mandate for delivering Citizen Services.

B. Need for Information Security

State requires an information security policy for the following reasons.

a) Maintaining Confidentiality: Confidentiality of information is mandated by IT laws (IT Amendment Act 2008) followed by GoR. Different classes of information warrant different degrees of confidentiality. The hardware and software components that constitute the IT assets represent a sizable monetary investment that must be protected. The same is true for the information stored in its IT systems, some of which may have taken huge resources to generate, and some of which can never be reproduced.

b) Integrity & Availability: The integrity and availability of information, whether acquired, provided or created must be ensured at all times.

c) Safeguarding Critical Information: Critical information like audit reports, budgets, sensitive and confidential information is protected from unauthorized access, use, disclosure, modification and disposal, whether intentional or unintentional.

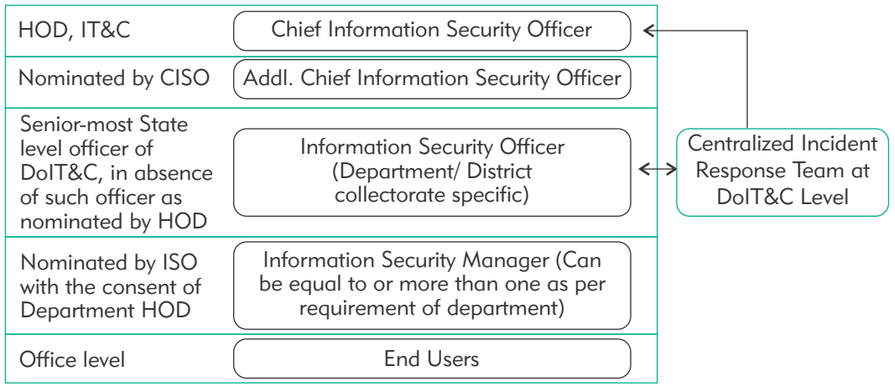
d) Awareness among officers and officials: officers and officials, third party users are made aware of the information security policy.

C. Review & Evaluation

The State shall be responsible for review and approval of Information Security Policy at the time of any major change(s) in the existing environment or once every year, whichever is earlier. Review shall take place in response to significant changes including but not limited to changes in risk assessment, security incidents, new vulnerability, change in technology or network infrastructure. The changes suggested in the Policy shall be approved from the appropriate authority and institutionalized within State with intimation to all concerned.

D. Information Security Organization Structure

Figure 1



a) Chief Information Security Officer (CISO)

The Chief Information Security Officer shall provide the direction and support for all information security initiatives. The CISO is responsible for providing direction and leadership through:

i. Reviewing and Approval of the Information Security Policy.
ii. Approval of the resource requirements (human, IT Assets and financial) for information security.
iii. Driving information security initiatives across GoR.
iv. Conducting status review(s) of security implementation at Government Departments.

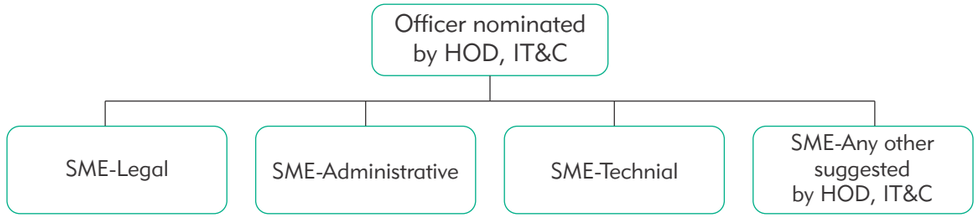
b) Additional Chief Information Security Officer (Addl. CISO)

i. Review the Information Security Policy periodically.
ii. Propose the resource requirements (human, IT Assets and financial) for information security.
iii. Prepare roadmap to drive information security initiatives across the State.
iv. Monitor security implementation at Government Departments.
v. Organize a refresher course for Information Security Officer with regards to Information Security.
vi. Prepare the classification of Information assets.
vii. Understanding and Circulation of all the IT laws and amendments to Concerned ISOs.

c) Incident Response Team (IRT)

Incident Response Team will be an independent body headed by officer nominated by HOD, IT&C. Members of IRT shall include Subject Matter Experts from all domains viz. legal, administrative, technical, etc.

Figure 2



The IRT will check the authenticity of security incident and shall forward the request to CERT-In for resolution and coordinate with them till the closer of incident.

An Incident Reporting Team shall be made responsible for root cause analysis of security incidents and to preserve the logs and details for legal actions collected during analysis and recommend the preventive and corrective action to ISO. This team will be established by DoIT&C.

d) Information Security Officer (ISO)

The ISO assumes overall responsibility for ensuring the implementation, monitoring, training and enforcement of the information security policy and standards within the department/ district collectorate office

i. ISO will be responsible for the implementation of the Information Security Policy and monitor the compliance by departmental officials.
ii. Recommending, coordinating and implementation of information security policies, standards, processes, training and awareness programs; to ensure appropriate safeguards are implemented.
iii. ISOs are responsible for ensuring that appropriate controls are in place on the IT Assets to preserve the security properties of confidentiality, integrity, availability and privacy of departmental information

e) Information Security Manager (ISM)

Information Security Manager of respective departments is responsible for:

i. Administering security tools, reviewing security practices, identifying and analyzing security threats and solutions and responding appropriately to security violations.
ii. Administration of all user-ids and passwords and the associated processes for reviewing, logging, implementing access rights, emergency privileges and reporting requirements.

f) End User

End User is responsible for following:

i. It is the responsibility of each end user to report any incident which is observed /suspected to ISM.
ii. Users shall not test any existence of vulnerability in the information systems.

iii. Understand the IT laws and amendments.
iv. Avoid breaches of any law, statutory, regulatory and/ or contractual obligations as well as security requirements.

6.2 Asset Management

A. Introduction

For information systems to be used effectively, efficiently and legally the assets that make up those systems must be properly controlled. This is referred to as asset management.

Asset management is not limited to stock of information (electronic data) but also covers physical computer equipment's/Softwares used to access them. This Policy shall emphasize on the importance of identification /classification of IT assets to ensure adequate accountability and responsibility of the ISO/ISM. The Policy also ensures that information systems needs to be suitably protected based on the confidentiality, integrity and availability of the information systems.

B. Responsibility

ISM shall be made responsible for following:

a) A computer-based Asset Register shall be prepared and maintained for recording all Information Assets with their appropriate classification.
b) Providing Asset Management reports to user department as and when required on approval from ISO.

C. Ownership

ISO shall ensure that Information assets belonging to department has been identified and documented. The ISO shall be responsible for following:

a) Ensuring that all the Information assets are recorded in asset register
b) Establishing the classification scheme of the Information assets.
c) Implement appropriate security controls to safeguard the Information assets as per Information Security Policy.
d) Review and update the asset register to reflect any changes to the access rights

and or the classification scheme of the IT asset.

D. Information Classification

All information assets will have different degrees of sensitivity and accessibility to the organization. Information shall be classified appropriately as applicable for each department into the following categories:

a) Secret: This is applied to information unauthorized disclosure of which could be expected to cause serious damage to the National/State security or National/State interest. This classification should be used for highly important information and is the highest classification normally used. E.g. Visits of VIPs, security arrangements during VIP visits and international events, information related to critical infrastructure such as configuration details of servers in data centres, etc.
b) Restricted: This shall be applied to information, unauthorized disclosure of which could be expected to cause damage to the security of the department or could be prejudicial to the interest of the department or could affect the department in its functioning. The information that is used as official information for departmental level only (Restricted Circulation), etc.
c) Public: Information available in public domain like Government websites etc.

It is the responsibility of the ISO to appropriately classify their assets. The classification process shall be completed for existing assets and shall be undertaken for any new project at the time of deploying a new asset or generation of information.

6.3 Data and Information Security

A. Introduction

The Data and Information Security ensures that the officers and officials, contractors, consultants and vendors who have access to GoR information and associated Information assets understand their security responsibilities that are required to maintain the protection of critical information and the controls that are required to protect the information assets from human error, theft, fraud and/ or their misuse are implemented.

B. Objective

All officers and officials, contractors, consultants and vendors who have access to GoR information and associated IT assets are required to understand and practice their responsibilities for the comprehensive protection of the information assets. Failure to adhere to information security responsibilities may entail appropriate disciplinary action as per Rajasthan Service Rules, Government of Rajasthan.

The objectives of this Policy are to:

a) Ensure that the officers and officials, contractors, consultants and vendors understand their roles and responsibilities regarding information security.
b) Reduce the risks of human error, theft, fraud or misuse of the information assets.
c) Ensure that employees are aware of information security threats and concerns.
d) Minimize the damage from the security incidents and malfunctions and learn from such incidents.

C. During Employment

ISO has the following responsibilities during employment of officer/official:

a) The employees are made aware of their security responsibilities to maintain the information security.
b) An adequate level of awareness, education and training on the information security is provided to all employees.

D. Information Security Awareness and Training

The ISO in consultation with CISO shall ensure that:

a) Officers and Officials receive appropriate training on information security requirements.
b) Officers and Officials are made aware of disciplinary process, which can be initiated against them in case of any violations of this Policy.
c) Posters and hand-outs are used for creating security awareness among Officers and Officials
d) Quiz, tests, questionnaire are circulated to measure the awareness of Officers and Officials relating to information security on periodic basis.

E. Reporting Information Security Incidents

a) Officers/Officials who become aware of any loss, compromise of information or any other incident, which has information security implications, shall immediately report to the ISM.
b) Suitable feedback processes shall be implemented by Incident Response Team to ensure that the person reporting the incident is informed about the results after the incident has been investigated and closed in consultation with concerned ISO and ISM.
c) Security incidents shall be documented and used in user awareness training as learning from incidents.
d) End Users shall be informed that they should not, in any circumstances, attempt to prove a suspected weakness. Any action in testing the weakness would be interpreted as a potential misuse of the system.

F. Disciplinary Action

The certain categories of activities, which have potential to harm, or actually harm the information assets are defined as security violations and are strictly prohibited. The security violations may entail a disciplinary action. Appropriate disciplinary action can be taken against security violations as per Rajasthan Service Rules, Government of Rajasthan.

G. Termination or Change of Employment

a) ISM shall ensure that officers and officials are communicated about their information security responsibilities even after termination of employment/ contract regarding the return of all issued software, documents, equipment, mobile computing devices, and access cards, manual and/ or any other asset that is a property of GoR.
b) The ISM is required to ensure that the access rights of the officers and officials for information assets are removed upon the termination of his employment, contract or agreement.
c) The ISM is required to ensure that in case of change of responsibility, the access rights are revoked or modified as required and appropriate with proper approval from ISO.

6.4 Physical & Environmental Security

A. Introduction

The Physical and Environmental Security provides direction for the development and implementation of appropriate security controls that are required to maintain the protection of information systems and processing facilities from physical and environmental threats. Information systems should be physically protected against malicious or accidental damage or loss, overheating, loss of mains power, etc.

B. Objectives

Adequate protection shall be provided to information systems and facilities against the unauthorised physical access and environmental threats. Appropriate security controls shall be implemented to maintain the security and adequacy of the information systems and equipment.

C. Physical Security Parameter

ISM is required to define the physical security perimeter for concerned department and facilities where information systems of Government of Rajasthan are available. It is strongly recommended that the physical access restrictions proportionate with the criticality value of information system is implemented at perimeter of all such facilities where information assets are hosted.

D. Physical Entry Controls

a) Access control system shall be installed at key/critical locations of Govt. departments.
b) Access to Govt. department, facilities and secure areas (such as Data Centre, Development Centre) shall be provided to authorised personnel only. Access to secure areas shall be controlled and monitored.
c) All premises and facilities, where information assets are hosted, shall be classified into zones with defined security controls.
d) Zones should be designed and managed to protect against unauthorised access, detect attempted or actual unauthorised access and activate an effective

response.
e) Some areas are open to general public, whereas some areas may be restricted to few officer and officials strictly on need basis like public, internal and restricted.

E. Public Access, Delivery and Loading Areas

a) It shall be ensured that all areas, where loading and unloading of items is done, are monitored and equipped with the appropriate physical security controls during these activities.
b) Access to these areas shall be confined only to the identified and authorised personnel.
c) The movement of all incoming and outgoing items shall be documented and incoming items shall be inspected for the potential threats.
d) It shall be ensured that all the outgoing items have a valid authorisation and gate pass.

F. Equipment Security

Information Security Manager (ISM) in consultation with ISO shall implement the equipment security controls to prevent loss, damage, theft or compromise of information systems.

Critical IT equipment, cabling, ect. should be protected against physical damage, fire, flood, theft, etc., both on- and off-site. Power supplies and cabling should be secured. IT equipment should be maintained properly and disposed of securely.

G. Equipment Location and Protection

All equipment shall be protected against environmental threats and unauthorised access. It shall be ensured that:

a) The equipment are appropriately located and security controls are implemented to reduce the risk of potential threats (e.g. theft, fire, smoke, electrical supply interference) for their continued operations.
b) The unattended equipment such as servers, network are placed in secure enclosures.
c) The appropriate environmental protection controls are identified and implemented

for the safety of the equipment.

H. Power Supplies

All equipment shall be protected from the power failures and other disruptions caused by failures in supporting utilities. ISM & ISO shall jointly ensure that:

a) All supporting utilities, such as electricity, water supply, sewage, heating/ventilation and air conditioning, are in appropriate condition for the information systems and/or processing facilities that they are supporting.
b) The uninterruptible power supply (UPS) systems and generators are installed to support the continued functioning of equipment supporting critical business operations.
c) UPS equipment shall be maintained in accordance with the manufacturer's recommendations.
d) All department premises shall have proper earthing to prevent electric surges.
e) An alarm system to highlight the malfunctions in the supporting utilities is installed.
f) Voltage regulators shall be installed, wherever necessary, to guard against fluctuations in power. Circuit breakers of appropriate capacity shall be installed to protect the hardware against power fluctuations or short circuits.
g) A preventive maintenance exercise is carried out at regular intervals for the utility equipment.

I. Cabling Security

It shall be the responsibility of ISM to ensure that cabling is done properly. Following controls shall be considered for cabling security:

a) All cables, including power and telecommunication network cables, shall be protected from the damage or unauthorized interception.
b) All network cables and their corresponding terminals shall be identified and marked.
c) It is strongly recommended that the documents, including detailed physical network diagrams showing cable routings and terminations are maintained with ISM.

d) It shall be ensured that the power cables are segregated from the communication cables.

J. Equipment Maintenance

ISO shall ensure the following controls for equipment maintenance:

a) A preventive maintenance exercise for the utility equipments shall be conducted in scheduled intervals ensuring their continued availability and integrity.
b) Preventive maintenance of hardware, UPS, AC and other equipment shall be covered under AMC.
c) The ISM shall monitor SLA to ensure that preventive maintenance is carried out in efficient manner.
d) ISM is required to apply the appropriate security controls to the off-site equipment considering various risks that may exist outside the premises.
e) Every user is required to ensure that the equipment and information systems are disposed of after an approval from the ISO and following proper rules as per Government of Rajasthan Rules for disposing IT Assets.
f) Any equipment, information system, storage device or software under the possession of or having information of State Government department shall not be taken outside the office premises without prior authorization of ISM and valid gate pass.

6.5 Communication & Operations Management

A. Introduction

The Communication and Operations Management establishes appropriate controls to prevent unauthorized access, misuse or failure of information systems and equipment and to ensure the confidentiality, integrity and availability of information that is processed by or stored in the information systems/equipment.

B. Responsibility

The ISM is responsible for the implementation of the controls defined in this Policy. However, ISO shall ensure compliance of Information Security Policy.

C. Objective

Government of Rajasthan shall ensure the effective and secure operation of its information systems and computing devices. The objectives are to:

a) Develop documented operation procedures for information systems and computing devices.
b) Ensure protection of information during its transmission through communication networks.
c) Protect integrity of software and information against the malicious codes.
d) Develop an appropriate backup strategy and monitoring plan for protecting integrity and availability of information processing facilities and communication services.
e) Have appropriate controls over storage media to prevent its damage and/or theft.
f) Maintain security during the information exchange with other State Governments.

D. Operations Procedures and Responsibilities

IT operating responsibilities and procedures should be documented. Changes to IT facilities and systems should be controlled. Duties should be segregated between different people where relevant (e.g. access to development and operational systems should be segregated).

E. Documented Operating Procedure

a) Adequate documentations shall exist for maintenance of information systems. The documentations, procedures and checklists shall be created when a new systems or service is introduced and the activities to be carried out when a service failure occurs or when maintenance needs to be performed.
b) Procedures shall be in place to ensure that activities performed in day-to-day operations are carried out in a secure manner.
c) Standard Operating Procedure (SOP) shall be created to maintain the confidentiality, integrity and availability of that specific platform or application.

F. Change Management and Change Request Approval

For application software the documentation shall provide for a brief description of the changes requested, date on which the request was made, prioritizing of the request, tracking and controlling modifications and assigning a unique number to each request. All changes requested shall be approved/rejected by ISO of concerned department.

G. Hardware and Operating System Changes for Information Systems

a) Any changes to hardware shall be done by raising a change request, approval by the ISO and documentation of the same.
b) ISM shall update the asset register once the changes are done to the hardware.
c) Any change to the operating system or application shall be strictly controlled. Any changes shall be done by raising a change request, approval by the ISO and documentation of the same.

H. Testing of Changes and Backup

a) All critical and complex changes shall be tested before being carried out in the live/production environment.
b) A quality assurance test of the changes to be implemented shall be performed in a test environment prior to implementation in the production environment.
c) A backup of the system impacted by the change shall be made prior to its being updated.

I. Unscheduled/Emergency Charges

a) Unscheduled/emergency changes shall be carried out only in case there are critical issues in current IT system/ environment, which require the change to be carried out with approval from ISO
b) An audit trail of the emergency activity shall also be generated which logs all activity, including but not limited to:
    I. The user-ID making the change
    ii. Time and date
    iii. The commands executed

iv. The program and data files affected

J. Segregation of Duties

Segregation of duties is important in order to reduce opportunities for unauthorized modification or misuse of information, or services.

a) ISM shall segregate the duties in such a manner so that no single user has the ability to subvert any security controls of the infrastructure thereby negatively impacting the business operations.

b) An individual shall not be responsible for more than one of the following duties: data entry, computer operation, network management, system administration, systems development, change management, security administration, security audit, security monitoring.

Whenever segregation of duties is difficult to accomplish, other compensatory controls such as Monitoring of activities, Audit Trails and Management Supervision can be implemented.

K. System Planning and Acceptance

For maintaining adequate future storage and memory demands of IT Systems proper monitoring and requirement projection is performed for information assets. This will help in avoiding potential bottlenecks that might present a threat to system security or user services.ISM will identify the requirement and will send the requirement to ISO. ISO will review the same and will further send it to approving authority.

L. Protection against Malicious and Mobile Code

ISM shall ensure to implement software and associated controls to prevent and detect the introduction of malicious and mobile codes like Computer Virus, Trojan Horse, etc. which can cause serious damage to networks, workstations and critical Government data.

Mobile code is any program, application, or content capable of movement while embedded in an email, document or website. Mobile code uses network or storage media, such as a Universal Serial Bus (USB) flash drive, to execute local code execution from another computer system. The term is often used in a malicious

context; mobile code creates varying degrees of computer and system damage. Mobile code is usually downloaded via the body of an HTML email or email attachment. Therefore in the information systems where the use of mobile code is authorised, ISM shall ensure configuration in such a manner that only authorized mobile code operates according to a clearly defined set of rules.

M. Backup

For continuity of business operations in the event of failures and/ or disaster, it is essential to have the secondary copies of the data available. It is to be ensured that backups of all the identified highly critical information assets are taken and are tested for restoration and readable or regular intervals.

Information Security Manager is required to ensure following:

a) Identification of critical information assets

b) Selection of appropriate backup media on the criticality of data and retention period

c) Backup logs shall be regularly maintained and kept up-to-date and can be in the form of hard or soft copies

N. Network Security Management

a) Network Controls

The appropriate security controls shall be implemented by the ISM to protect the departmental network. The controls shall include, but not limited to, the following:

i. Logical segregation of networks e.g. internal network zone, Demilitarized Zone (DMZ) and External zone

ii. Protection through firewall

iii. The Documentation related to the network diagram, IP Addressing and configuration of network devices, etc.

b) Wireless Local Area Network (WLAN)

The wireless infrastructure system shall be managed appropriately in order to provide protection to its information and information systems. The following controls shall be implemented by ISM to ensure WLAN security:

i. Secure configuration of wireless communication devices including the Access

Points and wireless client devices such as Laptops/Workstations.

ii. Implementation of a strong key management system for the authentication of clients connecting to the WLAN.

iii. Implementation of appropriate physical and environmental security controls to protect wireless access points against theft and damage.

iv. Register access points and cards. All wireless access points must be registered and approved by ISM. These access points are subject to periodic penetration tests and audits.

c) Firewall

ISM shall establish following controls:

i. Firewalls shall restrict access to all applications and network resources and protect these from unauthorized users

ii. Access control policy shall be implemented on the Firewall and all activities shall be logged (successful, unsuccessful)

iii. Publicly accessible servers shall be kept behind the Firewall and access control policies shall be defined

iv. An updated, reviewed and approved network diagram with all connection to and from the firewall shall be maintained.

v. A documented list of services and ports shall be maintained.

vi. Approval process for new rules for firewall shall be established

d) Security of Network Services

I. The ISM is required to identify the security features, service levels and management requirements of all network services included in any network services agreement, irrespective of the fact whether these services are being provided in-house or outsourced.

ii. The ISM shall prepare a checklist of the non-essential, default and vulnerable services for all the information systems owned by them. The non-essential services shall be disabled on all information systems and the default and vulnerable services required for business operations shall be fixed by implementing alternative mitigation controls on the information systems.

O. Exchange of Information

a) Information Exchange

Appropriate security controls shall be implemented to exchange the Govt. department information or software assets with third parties. The security controls shall include technical controls and contract/agreements signed with the third parties.

The relevant information asset owners/ISM/ISO shall be responsible for ensuring that such information assets are exchanged only after signing appropriate agreements.

P. Monitoring

a) ISM needs to ensure that proper logs are maintained and stored for a specific time period for future investigation purposes.

b) Audit logs shall be secured in such a manner that even the ISO/CISO is not allowed to erase or modify the logs of the activities performed by them on system.

c) Access to Log shall only be provided on need basis and with approval from ISO.

d) Time and date synchronization shall be maintained at all network devices and servers.

6.6 Access Control

A. Objective

User Access of the Information assets shall be based on their roles and responsibilities provided. All the User ids are provided with access permissions as per requirements, role and designation of officers and officials. The system shall deny all request other than permitted to protect the information from unauthorised access.

The objectives of the Access Control are to:

a) Provide need-based access to information assets

b) Prevention of unauthorised access to information systems, network services, operating systems, databases, information and applications

B. User Access Management

The allocation of access rights to users should be formally controlled through user registration and administration procedures (from initial user registration through to removal of access rights when no longer required), including special restrictions over the allocation of privileges and management of passwords, and regular access rights reviews where if roles and responsibilities change for officers and officials than his access rights shall be changed accordingly.

a) Users shall be provided access as per their roles and responsibilities, e.g. DDO is provided access to disburse salaries of his concerned office but is not allowed to view or disburse salary for other offices.
b) Unique User id shall be provided to each employee so that each person will be responsible for one's action which will help in tracking of security threats incidents, if any.
c) User rights shall be provided by system administrator on written approval from ISM/ISO of Concerned department.

C. User Registration

a) Documentation and implementation of procedures for registration and de-registration of User id.
b) Naming Convention shall be followed for User id creation
c) Identification of inactive accounts and disabling them
d) Re-activation of the accounts on written request from ISM
e) Guest accounts to be disabled on servers

D. Password Management

a) It is made mandatory for users to change their passwords during the first time logon and after 20 days of each password change. Warnings to the users shall be flashed before 5 days of the password expiry and to be sent repeatedly everyday till the user changes password or password expires.
b) The Password shall have a combination of alpha-numeric characters and minimum length of eight characters for strong security.
c) System shall keep record of last five passwords and shall not allow user to reuse it at the time of changing one's passwords

d) After maximum 5 unsuccessful login attempts, account shall be locked for security purposes.
e) The passwords shall not be hard coded into the logon scripts, batch programs or any other executable files when user authentication or authorisation is required to complete a function.
f) The password shall be encrypted while transmitting over network.
g) For forgot passwords and account lockouts, proper support procedures shall be documented and implemented.
h) User password reset is performed only when requested from user and after identifying and verifying the user through defined procedures.

E. User Responsibilities

All Users who will have access to information assets of Government of Rajasthan are required to understand their responsibilities for maintaining the effective Security Controls and safety of information assets.

F. "Clear Desk and Clear Screen" and "Security of Unattended Equipment"

IT team needs to ensure that information system needs is auto locked if unattended for a specified duration

a) Sensitive and critical information need to be locked (electronic media)
b) Desktops shall be logged off or protected with a screen when unattended for a specified duration.
c) Incoming and outgoing mail points should be protected.
d) Use of scanner and digital cameras shall be monitored so that unauthorised use for reproduction of critical information can be prevented.
e) Logout from the workstation, servers and/or network device when the session is finished.

G. Application and Information Access Control

The logical access to the application software shall be restricted to the authorised users only. The access rights shall be provided for relevant section of application, e.g. DDO is provided access to prepare salary bills for one's concerned office employees.

a) User access matrix shall be updated quarterly and documented
b) Information systems (Application system processing) containing critical information shall not be hosted on the shared server, and
c) High level logging mechanism shall be established for critical systems.

H. Mobile Computing and Communication

a) Employees shall be allowed to remotely access GoR network to access official information after proper identification and authentication.
b) The employees shall take special care of the mobile computing resources such as, but not limited to, Laptops, mobile phones, PDA's, etc. to prevent the compromise and/or destruction of confidential information.
c) Official laptops shall be configured as per policy with proper firewall and updated virus definitions to secure the information systems

6.7 Information Security Incident Management

A. Objective

All the security breaches, discovered weakness in the system and attempts to breach in the Information systems shall be reported and responded to promptly. Appropriate actions shall be taken to prevent the reoccurrence.

The objectives are to:

a) Develop proactive measures so that the impact of any security incident on information systems can be minimized
b) Create awareness among users so that they can report the identified incidents to ISM.
c) Get learnings from the incidents and implementing appropriate controls to prevent the reoccurrence

B. Incident Identification

An incident is the act of violating the security policy defined for State. The following actions can be classified as incidents, but not limited to:

Category	Nature	Description
Cat 1	Unauthorised Access	Attempts to gain unauthorised access to a system or its data without having permission, e.g. spoofing as authorised users
Cat 2	Denial of Services	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources.
Cat 3	Malicious Code	Successful installation of malicious software (virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.
Cat 4	Changes to Information System	Changes to system hardware, firmware or software characteristics and data without the application owner's knowledge.
Cat 4	Changes to Information System	Changes to system hardware, firmware or software characteristics and data without the application owner's knowledge.
Cat 5	Unknown User Accounts	Existence of unknown user accounts
Cat 6	Others, if any	Any other incidents identified by users

C. Reporting Security Events and Weakness

a) An incident management procedure shall be formalized and documented which includes incident identification, reporting, response, escalation and incident resolution.
b) There should be a central point of contact (ISM), and all employees/users should be informed of their incident reporting responsibilities.
c) Users shall not test existence of any vulnerability in the information systems

D. Learnings from Information Security Events

A knowledge base shall be established by IRT for the information gained from the evaluation and analysis of all information security incidents, that will be helpful to prevent reoccurrence of security incidents, to handle security incidents and for learning.

E. Collection of Evidence

a) As per the legal requirements, ISO shall collect the evidences during the incident analysis, retained and presented for relevant jurisdiction. IRT will provide complete

help to ISO for collection of evidence. IRT has to preserve the proof for any legal proceedings to support ISO.

b) Delayed reporting of information security events or incidents, and consequent delays in initiating investigations can result in loss of evidence. Therefore, timely investigation shall be performed by IRT.

c) Evidence shall be collected in such a manner that it should not destroy its evidentiary proof and can be used for legal use in court, if required.

6.8 Compliance

A. Introduction

The Compliance provides the direction to design and implement appropriate controls to meet the legal, regulatory and contractual requirements as per Cyber law, IT Act 2000 and any other relevant act prevailing in India.

B. Responsibility

It is the responsibility of ISO to ensure implementation of the appropriate controls to meet the legal, regulatory and contractual requirements as circulated by ACISO. The details about the Cyber laws, but not limited to, is available at http://deity.gov.in/content/cyber-laws

C. Objective

All Government Departments shall understand the importance of Compliance to the legal requirements and thus enforce the appropriate controls to the officers and officials working under their department to embed a compliance culture.

The objectives are to:

a) Promote a positive ethical and compliance culture among Government offices

b) Creating awareness among users regarding the law compliance

c) Avoiding breaches of any law, statutory, regulatory and/ or contractual obligations as well as security requirements

d) Ensuring that officers and officials, third party users understand and adhere to the legal, statutory, regulatory and contractual requirements which may have an

impact on their daily activities

D. Compliance with Legal Requirement

a) Identification of Applicable Laws

It is the responsibility of ISO to maintain a list of all relevant statuary, regulatory and contractual requirements with the help of ISM in guidance of ACISO (Circulated by ACISO)

b) Intellectual Property Rights

i. All Software and application used in Government offices shall be purchased and issued in accordance with the license agreements.

ii. All employees shall abide by the Copyright laws detailed by the software vendor

iii. Awareness campaigns shall be organized for employees regarding IPR

iv. Software shall be used for official purpose only

v. Officers and Officials shall not be allowed to carry Personal Information Processing equipment or CD writers, USB drives, etc. without obtaining prior approval from ISM.

c) Protection of Government Records

i. Important records like accounting and financial records, payroll and other employee related records shall be protected from loss or destruction.

ii. Retention period shall be defined for various types of records as per rules and regulations and shall be destroyed in a safe and secure manner on completion of their retention period.

iii. Extra Protection shall be taken to store the records required to meet legal requirements.

d) Data Protection and Privacy of Personal Information

i. Personal information of employees/users shall be kept safe and confidential.

ii. Relevant Legal laws, Acts and regulations shall be followed for handling personal information.

iii. Personal records shall be retained and stored as required by legislation.

iv. The review period and review rights of personal records shall be defined by ISO.

v. Backup of personal records shall be ensured.

e) Prevention of misuse of Information Processing Facilities
   i. Users shall be prevented from accessing information, information systems and/ or facilities for unauthorized purposes through implementing appropriate access controls.
   ii. Any usage of information system other than for official purposes shall be considered as improper use of the facilities and may lead to disciplinary action against user.

E. Compliance with Information Security

I. The ISOs shall ensure that the Policy is implemented in their respective departments, in turn ensuring the compliance.
ii. It shall be communicated to all employees officially through a Government order that compliance to Information Security Policy is mandatory and if any non-compliance is found, necessary disciplinary action can be taken against the employee.
iii. There shall be a regular review of compliance to the policies using Internal Audits. Any deviations shall be noted and communicated to the HODs as a part of the Internal Audit report.

F. Technical Compliance

i. Technical compliance check shall be carried out to identify vulnerabilities in the system and to check effectiveness of controls to prevent unauthorized access to information systems.
ii. Information systems shall be checked by ISM every six months for security and compliance with the security Policies.
iii. A schedule shall be maintained to ensure that vulnerability assessment and penetration testing is carried out at regular frequency.
iv. Technical compliance shall be carried out by experts.

6.9 Internet Security

A. Introduction

Internet security provides directions to the officers and officials to ensure that internet

usage in Government departments is legitimate and does not breach any security of information system, thus preventing the unauthorised use of internet.

B. Responsibility

ISM shall ensure compliance of the Policy. Controls shall be established by IT Team under guidance of ISM. Each employee/user shall take responsibility to follow Internet Security Policy.

C. Objective

Appropriate technological and user level controls need to be established for ensuring legitimate use of internet in Government departments to maintain the confidentiality, integrity and availability of the internet system.
Following are the objectives:

a) Rules to be defined so that each employee in Government departments shall use internet for legitimate purpose
b) To ensure that internet system shall not be misused.

D. Internet Usage

a) Access to internet
   i. Internet should be provided to users for official purpose.
   ii. Internet access shall be provided after approval from ISM.
   iii. Access to Internet shall be controlled by Proxy server and firewall.
b) Authorised and unauthorised access to internet
   i. Internet usage shall be restricted to serve employees for official/office related work and transactions.
   ii. Unauthorised use of Internet shall include, but not limited to:
      1. Using for personal entertainment, personal business or profit, and publishing personal opinions.
      2. Attempting to gain or gaining unauthorized access to any computer system
      3. Sending/receiving/viewing racial or sexually threatening email messages
      4. Sending, transmitting or distributing proprietary information, data or other confidential information.

5. Using Internet for non-official purposes and wasting computer resources like uploading and downloading large files
6. Introducing computer viruses, worms, or Trojan horses
7. Downloading obscene written material or pornography

c) Downloading and uploading of software
   i. Downloading and uploading of software is allowed only when permissions are granted from ISM.
   ii. Trial versions shall be deleted after expiry of trial period.
   iii. Periodic review of all desktop/laptops shall be done to ensure that no unauthorized software is installed.
   iv. Browsers are configured at workstations in such a manner that they should accept applets only from trusted sources.

d) Internet Security awareness
   Users shall be kept aware through trainings regarding the acceptable and legitimate use of internet, e.g. downloading the content from internet, downloading of applets for browsers, etc.

e) Website blocking
   Internal users shall be blocked at the proxy level from accessing websites which are deemed inappropriate as per the directions from the State Government.

f) Auditing, logging and monitoring
   i. Logging shall be maintained for all the attempts to access internet services
   ii. ISM shall review log files of proxy server on periodic basis

6.10 E-mail Security

A. Introduction

E-mail Security provides directions and controls to be established for legitimate use of e-mail account provided to the users and to protect e-mail system from vulnerability and modifications. E-mails originating from registered domain of Government department/PSU/Boards/Corporation and other autonomous bodies only shall be considered for official purpose.

B. Responsibility

An e-mail server administrator for registered domains of Government departments/ PSU/Boards/Corporations and other autonomous bodies is responsible to ensure that appropriate controls are kept in place for one's email server. Each user is responsible for complying with the E-mail Security Policy. ISM shall ensure that access rights of e-mail id shall be managed, e.g. on transfer of officers and officials their e-mail id which is as per designation is given to other officer/official after changing the password.

C. Objective

a) E-mail security is of prime importance and appropriate technological and user level controls shall be implemented to maintain confidentiality, integrity and availability of the e-mail system by respective e-mail server administrators.

b) The objective of the e-mail policy is to Establish the rules for the official use of the e-mail system and to adequately protect the information transmitted through the e-mails.

c) If any PSU/Boards/Corporations/Autonomous bodies are not able to follow e-mail Policy due to lack of appropriate infrastructure, it is suggested to open their employee's email-id on the domain (www.rajasthan.gov.in) by taking necessary approvals.

D. Authorized Use of e-mail

a) All e-mail messages generated from registered e-mail System of Government department/PSU/Boards/Corporation and other Autonomous bodies shall be considered to be the property of Government of Rajasthan.

b) Users shall not forward/redistribute any offensive or unsolicited material received from the external sources.

E. Prohibited use of e-mail

a) Users shall not use e-mail for raising charitable funds campaign, political advocacy efforts, personal amusement and entertainment.

b) Users shall not use e-mail for creation or distribution of any disruptive or offensive

messages, including offensive comments about race, language, gender, hair colour, disabilities, age, sexual orientation, pornography, culture, religious beliefs and practice, political beliefs or national origin.

c) Users shall not use e-mail for forwarding or sending messages that have racial or sexual slur, political or religious solicitations or any other message that could damage the reputation.

d) Users shall not use email for transmitting any data that potentially contains Viruses, Trojan horses, Worms, spywares or any other harmful or malicious program.

e) Users shall not use e-mail in connection with surveys, contests, chain letters, junk e-mail, spamming, or any duplicative or unsolicited messages.

F. User Accountability

a) Users shall not use any unauthorised Web-mail services for official purpose.

b) Users shall not share their e-mail account passwords.

c) Users shall choose strong passwords as per password policy.

G. User Identity

a) Misrepresenting, Concealing, suppressing or replacing another user's identity on an electronic communications system is prohibited.

b) The user name, email address and related information included with electronic messages shall reflect the actual originator of the messages.

c) At a minimum, the users shall provide their name and mobile numbers in all e-mail communications.

H. E-mail Administrator Accountability

E-mail Administrator is responsible for following:

a) All e-mails and content shall be scanned through authorized email scanning software

b) Open relay is blocked at all e-mail servers to prevent spamming

c) Content monitoring systems shall be installed at e-mail Servers

d) Antivirus definitions shall be kept updated at the gateway/server levels

I. Electronic Mail Encryption

The objective of e-mail encryption is to prevent the email content from being read by unintended recipients.

All electronic communications through the e-mail systems are not encrypted by default. Therefore, if sensitive information needs to be sent by e-mail System, encryption or similar techniques provided by the e-mail system shall be employed for the protection of information being transmitted.

J. Attachment and Virus Protection

a) E-mail Server administrator shall implement appropriate controls at e-mail gateway/server level to scan email attachments and delete malicious file extensions or viruses. E-mail administrator shall block documented malicious file extensions at gateway level.

b) E-mail virus protection and content filtering software shall be implemented at e-mail gateway/server level.

K. Public Representations

a) No e-mail messages related to State Government shall be used for advertisement purposes.

b) If users are suffering from excessive spams in their mail box from a particular e-mail id than they shall raise a security incident to their respective ISM.

L. Archival, Storage and User Back up

All official e-mail messages containing approval, work delegation, authorisation or handing over of responsibilities or similar transactions shall be archived for future official use by end user.

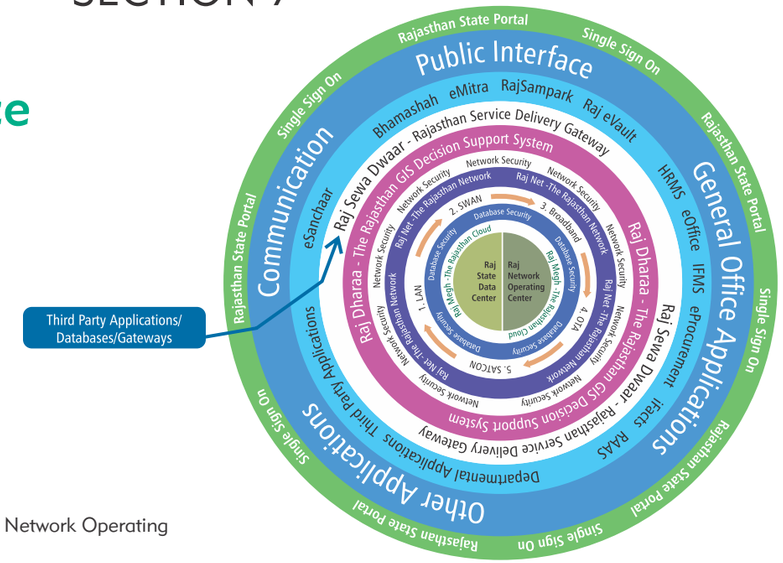
Any e-mail message which can be helpful as an evidence for critical decisions shall be appropriately retained for future use by end user.

M. Disclaimer

A disclaimer approved by CISO shall be appended to all e-mail messages generating from State Government domains.

SECTION 7

Rajasthan e-Governance Architecture



1. Rajasthan State Data Centre & Network Operating Centre:
   - 100 mbps Dedicated Connectivity;
   - Hosting more than 500 Websites, Portals and Applications
2. Raj Megh - The Rajasthan Cloud:
   - End-to-end Cloud enablement on SaaS, PaaS basis for Rajasthan
3. Raj Net - The Rajasthan Network:
   - Seamless connectivity till Gram Panchayat Level through LAN/SWAN/Broadband/Over-The-Air/Satellite
4. Raj Dharaa - The Rajasthan GIS-DSS:
   - A seamless Geographic Information System for Rajasthan, shared by all Government Departments, Organizations and utilized for systematic decision support.
5. Raj Sewa Dwaar - The Rajasthan Service Delivery Gateway:
   - Providing unique door of connectivity, unification and integration for all State, National and Private Applications/Gateways – The true Intelligent Middleware
6. Public Interface:
   1. Fully automated & mobile ready Solutions for
      - Public Interface (Bhamashah/eMitra/RajSampark)
      - Government officials (HRMS/eOffice/IFMS/eProcurement/ifacts)
      - Communication (eSanchaar)
   2. Raj eVault - Fully automated electronic verification, no need of hard copy documents/affedavits/notary attestation for service delivery
   3. RAAS (Rajasthan Accountability Assurance System) - End-to-End monitoring and accountability of government officials
   4. Mobile Apps for all Government portals & application on all plat forms
7. Rajasthan Single Sign On and State Portal:
   - One Person, One Identity – With all mapped datasets and documents for every state resident

सत्यमेव जयते

Government of Rajasthan
Department of Information Technology
and Communication

Resurgent
Rajasthan
PARTNERSHIP SUMMIT
19-20 Nov 2015 ▸ JAIPUR