Departmental Disaster Management Plan of Electronics & Information Technology Department, Government of Odisha

2019

OCAC Building, Bhubaneswar-751013

Preface

The Departmental Disaster Management Plan (DDMP) for the Electronics & Information Technology Department outlining the various measure to be taken in the event of any natural or man-made disaster during the year 2019 – 2020 has been prepared with a view to meet the challenges during Disaster.

The plan deals with Risk Assessment and Vulnerability Analysis, identification of Disaster Prone Areas, Inventory of Resources, Standard operating procedures, Detective and Corrective measures etc. The plan is prepared to help the E&IT Department and OCAC to focus quickly on the essentials and crucial aspects of both preparedness and response.

The Officials who are in-charge of different Electronics, IT and Telecom related activities of the department will remain alert to emergent situations that may arise in the course of the year.

A word of caution may be mentioned, however, plans are useful and work only if they are updated and practiced through intensive mock exercises and simulations.

Acknowledgement

The Departmental Disaster Management Plan (DDMP) for the Electronics & Information Technology Department would not have been possible without the kind support and help of multiple stakeholders, individuals and organizations. We would like to extend our sincere thanks to all of them.

Contents

Abbreviations and Acronyms

1. OCAC – Odisha Computer Application Centre
2. OSDC – Odisha State Data Centre
3. OSWAN – Odisha State Wide Area Network
4. STQC - Standardisation Testing and Quality Certification
5. TPA – Third Party Auditor
6. NMS – Network Management System
7. NOC – Network Operation Centre
8. CERT-In - Indian Computer Emergency Response Team
9. DR – Disaster Recovery
10. DMP – Disaster Management Plan
11. RPO - Recovery Point Objective
12. RTO - Recovery Time Objective
13. RAT - Risk Assessment Team
14. CMT - Crisis Management Team
15. DAT - Damage Assessment Team
16. ORT - Operations Recovery Team
17. CCTV - Closed-circuit television

Executive Summary

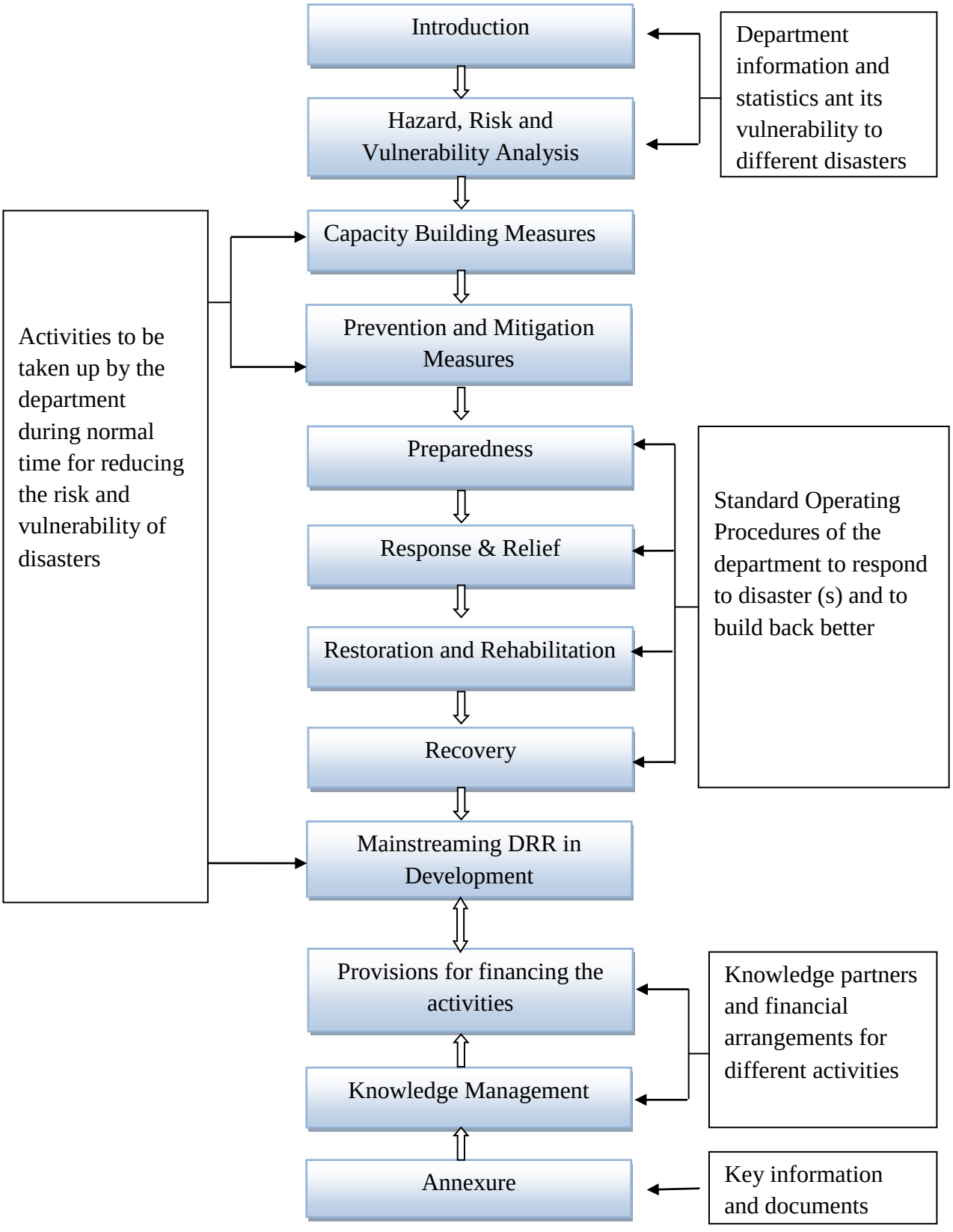
The DDMP (Departmental Disaster Management plan) of E&IT Department is in essence, the Standard Operating Procedure (SOP) in which the implementation of efforts is well laid down.

The DDMP aims at the following:

- Evolve an effective warning mechanism
- Identify activities and their levels
- Specify authorities for each level of activity
- Determine the response time for each activity
- Workout individual plans of each specified authority to achieve activation as per the response time.
- Have quick response teams
- Undergo preparedness drills.

The Disaster Management Plan for the department will be reviewed on quarterly basis and necessary updation as per the new requirements shall be incorporated. The Disaster Management Plan is hosted on the department's portal for dissemination of the information among the other departments and general public.

How to use the plan



Chapter – 1: Introduction

[*Declaration by the department that the Departmental Disaster Management Plan has been prepared as per the DM Act- 2005]*

As per the section 40(1) of Disaster Management Act, 2005, every department of the State Government, in conformity with the guidelines laid down by the State Authority, shall-

(a) Prepare a disaster management plan which shall lay down the following:-

i. the types of disasters to which different parts of the State are vulnerable;
ii. integration of strategies for the prevention of disaster or the mitigation of its effects or both with the development plans and programmes by the department;
iii. the roles and responsibilities of the department of the State in event of any threatening disaster situation or disaster and emergency support function it is required to perform;
iv. Present status of its preparedness to perform such roles or responsibilities or emergency support function.
v. The capacity-building and preparedness measures proposed to be put into effect in order to enable the Ministries or Departments of the Government of India to discharge their responsibilities.

1.1 Objective:

The objective of the plan is to identify all common elements of response. This acts as a base plan for all response activities. It provides a frame work around which E&IT Department can outline their own activities for disaster response. Preparation and planning well in advance have been reflected throughout the plan. Planning and preparation have been given a lot of importance, as it is better to be totally prepared rather than go unprepared.

So the broad objectives of the Departmental Disaster Management plan are

i. To protect vital information and records stored in digital form in the facility at IT Centre, Secretariat and Odisha State Data centre (OSDC) at OCAC
ii. To secure the SDC, SWAN and Secretariat Network
iii. To safeguard and make available vital materials, supplies and equipment to ensure the safety and recovery of records from expected disasters
iv. To reduce the risk of disasters caused by human error, deliberate destruction, and equipment failures.
v. To be in preparedness to recover from major natural disasters like Earthquake, Cyclone, Flood etc.
vi. To ensure that the critical IT Infrastructures to continue in operation after a disaster with minimal down time
vii. To recover the lost or damaged records or information after a disaster

1.2 Scope of the Plan:

Scope of the plan is to ensure, Network and Server farm infrastructure at SDC, SWAN and Secretariat up and running with no or minimal down time during disaster and recovery of data after disaster with appropriate disaster recovery mechanism.

1.3 Over view of the Department (Departmental Statistic profile):

Government of Odisha has accorded priority to the development of the Electronics & Information Technology Sector. In order to hasten up the progress, a separate Department of Information Technology was formed on 15th March, 2000. After the shifting of Government's priority towards electronics sector the name of department re-designated as Electronics & Information Technology department in 2016. Since then the Department of Electronics & Information Technology started functioning and now it is operating from OCAC building at Bhubaneswar. The department is being headed by Shri C.J. Venugopal, IAS, Principal Secretary. Odisha Computer Application Centre (OCAC), the designated Technical Directorate of Electronics & Information Technology Department is the nodal agency on behalf of the Department to implement e-Governance projects, provide IT solutions to various Departments of the state and create IT infrastructure like SWAN, SDC and SEC-LAN.

1.4 Acts, Rules and Policies governing the business of the department:

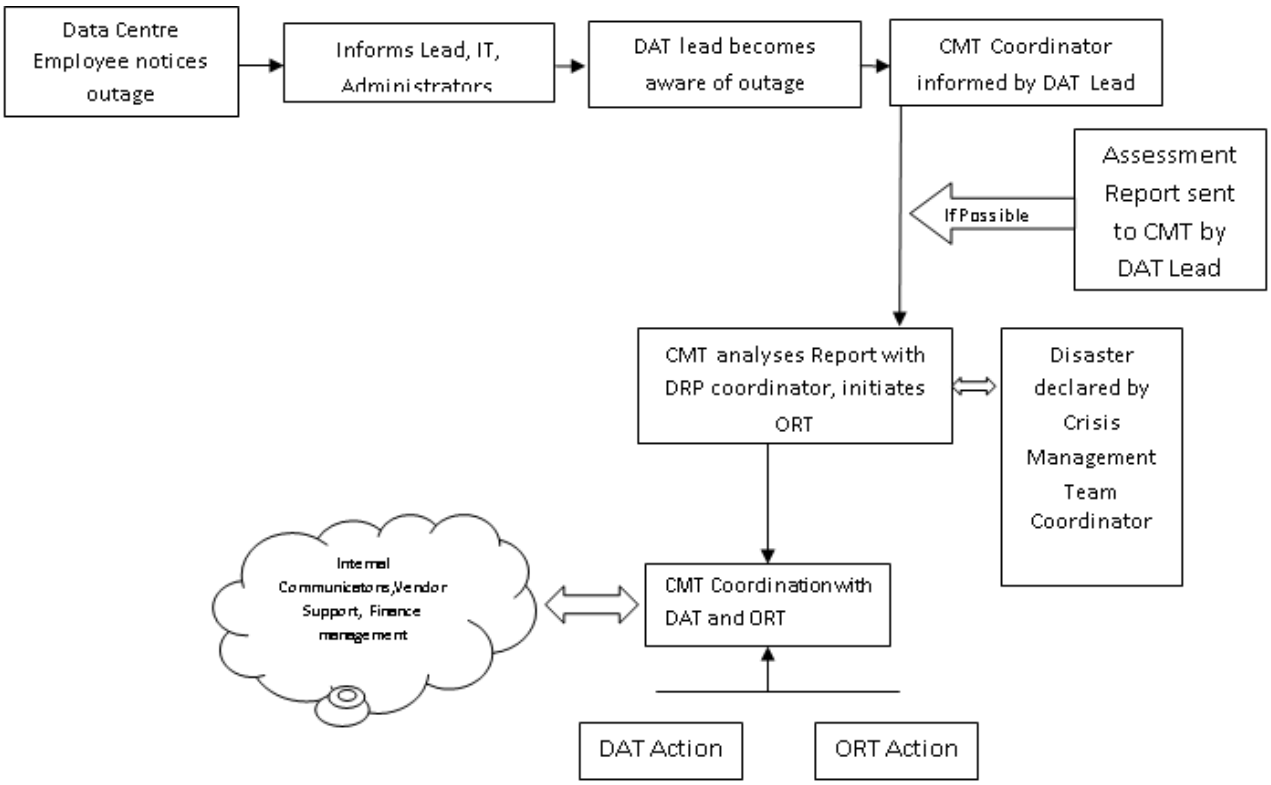
The business of the department is governed by Government rules and regulations besides IT ACT. The establishment is adapting the state crisis management plan and adhering to Cyber Security Policy.

1.5 Institutional Arrangement for Disaster Management (Organizational Structure)

i) Institutional Arrangement for IT Centre at Secretariat

- The establishment is being manually guarded 24 X 7 X 365 basis.
- Fire extinguishers have been installed at every sensitive location inside the establishment.
- Electrical and DG set; A/C Operators are available round the clock inside the establishment.
- All the equipments are under AMC with service level support within 2 hours.
- All the equipments are being checked up periodically so that in the emergency they will work flawlessly.
- Incremental Data backup is being taken twice in a day.
- Application back-up is being taken regularly.
- Stand by network equipments are available.
- Core and distribution switches are available in high availability mode.
- Redundant Internet Bandwidth is being taken from different sources to have high Internet availability and ensure at least one link is working during disaster.

ii) Institutional Arrangement for OSDC



1.6 Preparation and Implementation of the Departmental Disaster Management Plan.

Sl No.	Activities to be done	Timeline
1	Consultation within the department and with important stakeholders	2nd week of May
2	Finalization of the Departmental Disaster Management Plan at the Department level and submission of a copy to OSDMA	31st of May
3	Placing before State Executive Committee (SEC)	By June

****

Chapter – 2: Hazard, Risk & Vulnerability Analysis

2.1 History/ past disasters

2.2 Emerging Concerns

2.3 Hazard, Risk and Vulnerability Mapping

2.1 History/past disasters/losses in the department:

2.1.1 Causes of losses/damages;

[All disasters/ incidents that the department has faced during last 10 years to be mentioned below in tabular format. The department to keep the first 4 column intact and can modify the rest of the columns as per suitability to describe the loss and severity of the event.]

Table No. 01

Sl. No.	Year	Disaster event/ Incident	Location/ Affected districts/Area	Loss of Life	Damage to infrastructure	Other losses 1 (to be specified)	Other losses 2 (to be specified)
1	2012	State portal was defaced	State portal was defaced	No	No, restored within 2 to 3 minutes		
2	2013	Cyclone Phailin	No incidents happened and no loss or disruption of SDC services happened at the Primary Site	No	No, Adequate required steps were taken for smooth functioning of Data Centre.		
3	2014	Cyclone Hudhud	No incidents happened and no loss or disruption of SDC services happened at the Primary Site	No	No, Adequate required steps were taken for smooth functioning of Data Centre.		
4	2017	Minor Fire Hazard	No loss or disruption of SDC services	No	One Electrical circuit was damaged and replaced immediately		

2.2 Emerging Concerns:

Day by day more and more applications are being housed at IT Centre and there is no disaster management site. Hence if IT Centre is down many applications will not be accessed by public and intranet users. Possibility of hacking increases as more and more critical applications are hosted at site. No BMS is in place.

2.3 Hazard &Vulnerability Mapping:

2.3.1 Nature, frequency and intensity of disaster to which the department is prone to or is likely to be impacted in future;

All the threats mentioned below are potent to cause a Disaster. However, the Electronics & Information Technology Department is methodological in its approach to apply procedures like Fault Tolerance, and Information Security Management System controls, in order to prevent a risk from escalating to causing a Disaster.

Physical and Environmental Threats
Cyclone, Flood, Fire, Tsunami, Earthquake, Power Outage, Physical Security

IT Services Threats
Weak Data Back-up, Inefficient Storage Management, Weak Server Management, Vulnerable Operation Systems, Vulnerable Software, Virus / Spamming attacks, Inefficient security and communication link through the computer network, Cyber attack

Nature, frequency and intensity of disaster to which the OSDC (Odisha State Data Centre) is prone to or is likely to be impacted in future

Sl. No.	Incident	Level	Impact	Resources Affected	Result	Applicable Strategy
1.	Fire / Explosion	L3	Premises	People/ IT Infrastructure	Primary site not available.	S2
2.	Earthquake/Cyclone	L4	City Wide	People/ IT Infrastructure	Employee Shortage, Non Availability of	S2

Sl. No.	Incident	Level	Impact	Resources Affected	Result	Applicable Strategy
					Primary site for extended period	
3.	Power Outage	L2/L3	Premises	People/ IT Infrastructure	Primary site not available.	S2
4.	Air-conditioning failure	L1/L2	Premises	People/ IT Infrastructure	Primary site not available.	S1
5.	Political / Civil Unrest / Riots / Internal Strike	L4	City Wide	People	Most offices of city not accessible.	Remote Handling
6.	Theft / Unavailability of components	L2/L3	Premises	IT Infrastructure	SDC server systems affected	S1
7.	Heavy Rains / Floods	L3/L4	City Wide	People/ IT Infrastructure	Most offices of city not accessible.	Remote Handling, moving to S2
8.	Lightning / Storms	L3/L4	City Wide	People/ IT Infrastructure	Most offices of city not accessible.	Remote Handling, moving to S2
9.	Pests and Rodents	L1/L2	Premises	IT Infrastructure	Primary site not available.	S1
10.	Bombing / Acts of Terrorism	L3/L4	Premises/City Wide	People/ IT Infrastructure	Most offices of city not accessible.	Remote Handling, moving to S2
11.	Food Poisoning / Epidemic / Medical Emergency	L3/L4	Premises/City Wide	People	Employee Shortage	S1
12.	Virus Attack / Malicious Codes / Spam	L1/L2	IT Systems	IT Infrastructure	Application Level Disaster	S1
13.	Denial of Service	L1/L2	IT Systems	IT Infrastructure	Application Level Disaster	S1

Sl. No.	Incident	Level	Impact	Resources Affected	Result	Applicable Strategy
14.	Network Penetration / Hacking (Internal/ External)	L1/L2	IT Systems	IT Infrastructure	In worst case scenario, SDC Infrastructure not available	S1
15.	WAN Link / Communication Failure	L1/L2	IT Systems	IT Infrastructure	One or more premises affected	S1
16.	Hardware Failure	L1/L2	IT Systems	IT Infrastructure	SDC critical systems affected	S1/S2
17.	Software failure	L1/L2	IT Systems	IT Infrastructure	Minor outages	S1

2.3.2 Vulnerability of the department to various hazards.

Vulnerability of the Information System towards disasters, both natural and man- made is widely recognized. Natural Disasters can be though natural calamity and Man-made disasters could be intentional (for example, sabotage) or unintentional i.e that is accidental. It may involve Internet threats.

The need for an effective Information Technology (IT) disaster management strategy to lessen disaster impact is being felt in many quarters and also for strengthening of organizational structure for disaster management. Along with, regular updating of Disaster Plans on the basis of experience gained and use of various tools / technology should be done.

The intensity of a Disaster is a function of, which or how many of the critical resources are no longer available to provide defined services and its impact on the end user. Below are the IT services threats to OSWAN

- Disruption in communication links provided by BSNL.
- OFC cut during calamities.
- Disruption in equipment running due to power outage.

Below defined is the analysis of possible disasters to OSDC as per 4 levels of disaster intensity.

Level	Description
Level 1	**Failure impacting single Department** Significant malfunction of/disruption to primary infrastructure supporting operations of a single Department. e.g., Application failure
Level 2	**Failure impacting multiple Departments** Significant malfunction of/disruption to critical primary infrastructure, supporting operations of multiple Departments. For e.g., failure of any of the critical primary servers or data storage systems or network/security resource
Level 3	**Premises unavailable** Total shutdown of office infrastructure, as a result of fire, building collapse, bomb explosions etc. since the premises and equipments are inaccessible, people may have to congregate at an alternate location, if required.
Level 4	**Citywide disaster** Major impedance to employees trying to reach office or alternate office resources - e.g. due to riots, floods or other major citywide catastrophe.

2.3.3 Risk Analysis – calculating risk which various hazards/disaster can cause to department keeping in view its vulnerability and capacity

Infrastructure Available with the Department

a. Odisha State Data Centre (OSDC)
b. Secretariat IT Centre
c. Odisha State Wide Area Network (OSWAN)
d. Other ICT infrastructures like Servers, Desktop PCs, Softwares and Networking Equipments

Electronics & information Technology Department is taking preventive measures to prevent a disaster from occurring and those are designed to mitigate or prevent an event from happening.

****

Chapter-3: Capacity-Building Measures

3.1 Gaps in the Existing Capacity of the department

Lack of Domain experts especially in the field of Cyber Security.

3.2 Existing Human Resources in the department / OCAC trained on Disaster Management

Sl. no.	Category	Total Staffs	No of trained personnel on DM			
			Basic	ToTs	MoTs	Total
1	Administrative Staffs	15	Nil	Nil	Nil	Nil
2	Project Staffs	32	Nil	Nil	Nil	Nil
3	Accounts and Clerical Staffs	10	Nil	Nil	Nil	Nil
4	Support Staffs	11	Nil	Nil	Nil	Nil

3.3 Capacity-Building Plans

A). Electronics & Information Technology

Sl No.	Training Programmes on	Key Components/Topics	Target Audience
1	Awareness and Sensitization towards Cyber Security	Awareness and sensitization of all Government officials of Odisha towards impacts of Cyber Security and importance of its knowledge.	Officials of E&IT department, OCAC, SeMT, SDC Composite Team, Other department officials of Odisha, DeGMs and other district level officials

3.3.1 Capacity-Building Programmes at different level

3.3.2 State level Capacity-Building Plans;

Sl No.	Training for	Programmes
1	Additional Secretary, Joint Secretary, Deputy Secretary, Under Secretaries, SOs/ASOs	Training cum awareness programme at state level for better supervision, monitoring and taking preventive measures during Cyber Crisis.

3.3.3 District Level Capacity-Building Plans;

Sl No.	Training for	Programmes
1	DeGMs, DEOs, & other district level officers	Training programmes on effective management of Cyber Security, Disaster Management, Physical Security measures for IT

		Infrastructures etc.

3.3.4 Community level Capacity-Building Plans;

Sl No.	Training for	Programmes
1	DeGMs, IT Associations members, Manufacturers & Dealers of electronic products	Public awareness programmes. Distribution of relevant posters, leaflets, pamphlets in dual languages.

3.4 Training Need Assessment of the department

Sl. no.	Category	Types of Training Requires	Training Institutions
1	Policy Makers	Policy on Cyber Security	NIELIT / NISG / STQC / CERT-In
2	Technical Staffs	Cyber Security and Preventive measures	STQC / CERT-In
3	Administrative Staffs	Basic on Cyber Security & DM	NISG
4	Project Staffs	Basic on Cyber Security & DM	NIELIT / NISG
5	Accounts and Clerical Staffs	Basic on Cyber Security & DM	NIELIT / NISG
6	Support Staffs	Basic on Cyber Security & DM	NIELIT / NISG

3.5 Capacity-Building of Stakeholders and Beneficiaries of the department

a. Capacity building of all stakeholders will be done by E&IT Department.
b. The stakeholders are Officials of E&IT Department, OCAC, other departments of Odisha, Districts of Odisha etc.
c. The Officials will be trained on security measures to be adapted at the end point level to minimize internal threats and prevent disaster.
d. It has been planned to train at least 3 resources at IT Centre to tackle the disaster.

3.6 Requirement of funds for capacity-building programmes

Sl. No.	Training Programmes	Unit Cost	Total no. of Programmes	Total Cost
1.	Cyber Security and Preventive measures	1,00,000	2	2,00,000
2.	Physical Security measures for IT Infrastructures etc.	50,000	4	2,00,000
3.	Disaster Management	50,000	6	3,00,000

3.7 Annual training calendar of the department

Sl. No.	Name of the Course/ Training Programme	Participants	Duration of the Training Programme	Month of Organization	Training Institutions	Remarks if any
1.	Cyber Security and Preventive measures	Officials of E&IT department, OCAC, SeMT, SDC Composite Team, Other department officials of Odisha, DeGMs and other district level officials	3 days		NIELIT / NISG / STQC / CERT-In	
2.	Physical Security measures including Fire Hazards for IT Infrastructures etc.	do	2 days		NIELIT / NISG	
3.	Disaster Management	do	1 days		NIELIT / NISG	

3.8 Table top Exercises

N/A

3.9 Mock Drills

(Note: Details of Mock-drills of the department may be elaborated)

Sl. No.	Mock Drills on	Participants	Month of Organization	To be organized by	Remarks
1	Cyber Security	Nodal officers of all Departments	Jul' 2019	E&IT Deptt. in Association with CERT-IN	
2	Physical Security measures including Fire Hazards for IT Infrastructures etc.	Officials of E&IT department, OCAC, SeMT, SDC Composite Team, Other department officials of Odisha, DeGMs and other district level officials	Sept' 2019	E&IT Deptt & OCAC	

Chapter – 4:
Prevention & Mitigation Measures

4.1 Prevention & Mitigation Measures

- **Existing measures**

The three basic strategies that are being followed by the department are:

A. Preventive measures
B. Detective measures
C. Corrective measures

A. Preventive measures

Preventive measures are being taken to prevent a disaster from occurring. These measures seek to identify and reduce risks. They are designed to mitigate or prevent an event from happening.

These measures include:

- Business Impact Analysis for the selection of critical applications hosted in State Data Centre by gathering information on User Department processes and prioritizing the applications based on the impacts like Financial, Services, Target Citizen base, Legal and Regulatory. Criticality of all Applications shall be categorized into 3 classes, i.e Class I - Highly Critical, Class II - Critical, Class III – Not Critical Application specific data like the point beyond which data loss is not permissible i.e Recovery Point Objective (RPO) and the time within which the Systems/ Applications/ Functions must be recovered after an outage i.e Recovery Time Objective (RTO) will be known after this analysis.It will act as the basis for the development of appropriate backup strategies and suitable recovery strategies.
- Identification of Risks from various sources through Risk Assessment to identify which threat has the potential to cause more damage. The different parameters to be considered are :

Vulnerability - Indicating exposure of Information System resources to various threats.

Probability - Indicating the probability of a threat occurring.

Impact - Indicating impact of a threat on Information System resources.

- Data replication for web servers, data base servers, application servers and file servers at off site in SAN storage devices, DVD and Tape library
- Synchronization between State Data Centre and DR Site at New Delhi.
- Near line DR site for Secretariat data centre at State Data Centre in OCAC building.
- Testing the replicated/backup data through regular disaster recovery testing, mock drills to make sure that restoring backup data will be easy.
- Backup network operation centre (NOC) for OSWAN within Bhubaneswar
- Using diesel generator to avoid power outage at SDC, OSWAN NOC, BSNL exchange
- Conducting routine inspections, mock exercise and plan maintenance of Information systems both hard ware and software
- Centralized Antivirus software for ensuring virus free environment
- Security Audit of the Application at frequent intervals
- The storage media with data are being stored in fireproof safe locker and discarded backup media are disposed, so that data recovery is impossible.
- Deploying security personal for providing physical security
- Forming various Action Teams and fixing their Roles and Responsibilities like Risk Assessment Team (RAT),Crisis Management Team (CMT), Damage Assessment Team (DAT), Operations Recovery Team (ORT) and Help Desk
- The constituted Teams shall be lead by Special Secretary, E&IT Dept. Each team will have a designated Team Co-ordinator.
- Regular Disaster Recovery plan updations

Action Plan

The various task under preventive measures are to be taken by Risk Assessment Team which consists of members from –

- E&IT Department & Odisha Computer Application Centre (OCAC)

  (Special Secretary / Joint Secretary – E&IT Deptt., & Officer on Special Duty (OCAC) as Team Co-ordinator, DGM (Tech), System Analysts, Sr. Software Engineer, SeMT Consultants and others)
- Odisha State Data Centre (OSDC)

  (Project Manager & other Composite Team Members)
- Secretariat Data Centre (Head - State Portal, IT Centre, Secretariat, Bhubaneswar)
- Other Department's Official as on need basis

Operating Procedure

Sl. No.	Name of the Official	Role supposed to be played
1	Team Leader, Project Manager, SDC	Regular interactions with various Govt. Organisation like NIC, STPI, CERT-IN, DeitY, DoT, STQC, CDAC etc. and reputed private co. who have expertise in IT disaster management.
2	Team Members	Analyze the past history of IT disaster where it happens
3	Help Desk Team	Technical support to end user of the application
4	Team Members	Collect relevant intelligence available in reliable public domain like Government and private websites.
5	Team Members	Analyse the risk assessment sheet prepared for the Information Security Management System implementation for OSDC.

- **Drawing up of prevention & mitigation plans (disaster Specific)**

B. Detective measures

- Detective measures are being taken to discover the presence of any unwanted events within the IT infrastructure of the department like Odisha State Wide Area Network (OSWAN), Odisha State Data Centre (OSDC), Secretariat Data Centre and others.
- Aim is to uncover new potential threats. They may detect or uncover unwanted events.
- These measures include using fire alarms, using up-to-date antivirus software, firewall software, CCTV surveillance, holding employee training sessions, and using server and network monitoring software (NMS) for intrusion detection, network tomography, route analytics, website monitoring etc.

Action Plan

The various tasks under detective measures are to be taken by the constituted Team which consists of members from –

- Odisha Computer Application Centre (OCAC)
  (System Administrators, System Analysts and Sr. Software Engineers)
- Odisha State Data Centre (OSDC)
  (Project Manager & Composite Team Members)
- Secretariat Data Centre (Head, State Portal, IT Centre, Secretariat, Bhubaneswar)
- Implementing & Consulting Agencies (OSWAN Operator, Data Centre Operartor),Third Party Auditor (TPA), STQC, Government of India

Operating Procedure

Sl. No.	Name of the Official	Role supposed to be played
1	System Administrator, Sr. Software Engineer, SeMT Consultant	Discussions with various stake holders from Govt. and Private sectors to gain their expertise in advance monitoring of ICT resources and Application owners from the Department to suggest day to day monitoring mechanism required

2	System Administrator, Composite Team Members	Day to Day monitoring of various ICT resources of the Department using various Tools available like IBM Tivoli NMS for OSWAN and CA EMS for OSDC.
3	SeMT Consultant, Composite Team Members	Taking feedback from TPA & STQC and plan accordingly.
4	System Administrator, Composite Team Members	Put corrective measures in to action whenever any fault detected

C. Corrective measures

- Crisis Management Team (CMT) will swing in to action once disaster happens. It consists of Damage Assessment Team (DAT) members which will assess the affected Information Systems and Operations Recovery Team (ORT) members which will ensure that the IT Infrastructure is properly handled during the recovery process and the required resources are available on time.

- The focus of this Team is to recover the IT enablers supporting Information Systems critical business processes, to be up and running in concurrence with the identified Recovery objectives (RTO and RPO).
- Establishing a Help Desk which would play a crucial role in providing information proactively to various stakeholders.
- Taking the help of CERT-IN, the national nodal agency for any security incidents type of event occurred.
- To facilitate the efficient recovery and restoration of critical business functions, key staff members have been assigned different activities like Crisis Management, Damage Assessment and Operations Recovery, who will be put in to action once disaster strikes.

Action Plan

The various tasks under Corrective measures are to be taken by the constituted Team which consists of members from –

- E&IT Department and Odisha Computer Application Centre (OCAC)

(Special Secretary/Dy. Secretary/Under Secretary – E&IT Dept., Officer on Special Duty(OCAC), DGM(Tech), System Analysts & Sr. Software Engineers, SeMT Consultants and other officials)

- Odisha State Data Centre (OSDC)-Composite Team Members
- Secretariat Data Centre (Head, State Portal, IT Centre, Secretariat)
- Implementing Agencies (OSWAN Operator, Data Centre Operator and other SIs)

Disaster recovery strategies of SDC

Disaster recovery strategies are described below through a matrix that takes into account various scenarios i.e. any event that could disrupt the smooth functioning of the SDC:

Location of Manpower for Operations and Maintenance	Location of IT functioning Infrastructure	Whether a valid disaster scenario	Action
OSDC	SDC	No	Normal Operations
OSDC	NDC	Yes	S1
Other Site /NDC	SDC	No	Remote Handling
NDC	NDC	Yes	S2

From the table above, it can be seen that whenever the IT infrastructure at the NDC becomes the primary functioning candidate due to unavailability of the infrastructure at the OSDC, a Disaster may be declared. The Disaster Strategies to be adopted in turn shall be different for each kind of Disaster.

Below are the descriptions of such Strategies:

Scenario	Description
Scenario - I (S1)	**Operating from Primary site using DR infrastructure (No people movement).** This strategy is applicable when critical systems are unavailable at the Data Centre. However the Primary site is accessible and connectivity to the DR site is available. In such cases, the employees can remotely access and start the systems at DR site. Since, this would also involve some level of coordination between the personnel at the Primary and DR site; it is required to have relevant support at the DR Site. However, it must be ensured that critical data needed for Recovery is available at the DR site before system start up.

Scenario	Description
Remote Handling	**Operating from Remote logging using the infrastructure at Primary site** This strategy may be used in case of events like citywide disruptions which may potentially make the Primary site inaccessible to employees. The application systems are not affected at Primary infrastructure site and could be accessed from elsewhere (e.g. working from home). An SDC Disaster may not be declared in this case. This scenario involves active coordination from the Help Desk in getting the concerned team members connected through tele-conferencing, etc. This Strategy involves constant communication with the State Law enforcement teams. In case the SDC premise is expected to be affected, DR Strategy S2 can be initiated pro-actively after relevant communications among all stakeholders.
Scenario-II (S2)	**Operating from DR site using the DR infrastructure** This strategy may be used in case of a disaster that results in unavailability of the city hosting the Primary site (i.e. the premises, technology and infrastructure in the city hosting the Primary site are either unavailable or inaccessible). City wide disasters, terrorist attacks, etc. are some of the events that may result in such a failure scenario. Critical Departmental teams can work from home with DR site infrastructure in such scenarios.

The following table maps the possible recovery strategies to identify the intensity of event and various scenarios identified. However this list is not comprehensive and may need revision based on the learning of the Risk Assessment to be carried out at the SDC. The appropriate strategy will have to be selected based on the environmental conditions at the time of the disaster.

4.2 Ways & Means to prevent or reduce the impact of various disasters:

Structural Measures:

Sl. No.	Activity/ Project	Starting Date	Date of completion	Cost	Funding source	Out Come (persons to be benefited/ vulnerability reduction of area)

Non-structural Measures:

Sl. No.	Activity/ Project	Starting Date	Date of completion	Cost	Funding source	Out Come(persons to be benefited/ vulnerability reduction of area)

4.3 Hazard- Specific Mitigation Actions:

- To mitigate the Sea/ Water level rise, OSDC site built above the ground floor i.e. on second floor, OCAC Building.
- To mitigate the fire like situation, fire alarm with public address system installed to inform teams about the incidents. Also, fire extinguishers of different types installed on the floor at different location. Inside the server Fire suppression/ release (FM 200) gas was installed.
- For continuation of power supply two source of different distribution grid present at OSDC, still if in case of major power break down cause, 4 numbers of Diesel Genset installed with External Tanks for sufficient fuel holding to run the Genset(s) at the time of need.
- Daily Backup of all critical data of OSDC backed to DR site.
- To prevent theft cases, adequate required no of CCTV cameras are installed both inside and outside periphery for monitoring the OSDC premises. Round the clock Physical security
- To prevent from rodents, rodent repellent system installed inside OSDC.

***

Chapter – 5: Preparedness

This section should describe, in general, the capabilities and processes the department has in place to implement the range of preventive/ protective actions that may be required for various hazards. The preparatory activates listed below are activities that may be required to implement preventive/ protective actions in response to certain types of hazards.

5.1 Nodal person

Sl No.	Name & Designation of the Nodal person for Disaster Management in the Department	Contact No.	
		Office	Mobile
1.	Aditya Mohapatra , Joint Secretary, E&IT Department	0674-2567838	9437168606

5.2 Emergency Operation Center (Department)

Number of Staffs assigned	**Name of the staff**	**Specific Task Assigned**	**Contact No**	
			Office	Mobile
	A.K. Hota	Warning Communication	0674-2392870	9437633654
	A.K. Hota	Response & Relief	0674-2323074	9437633654
	A.K. Hota	Capacity Building	0674-2323074	9437633654
	S.K. Bhol	Capacity & Resource Development	0674-2567995	9938478383
	S.K. Bhol	Prevention & mitigation measures	0674-2567995	9938478383

5.3 Contact details of the Heads of the Department/Division

Sl No.	Name of the District/Division	Name of the Nodal /Head	Contact No	
			e-mail	Mobile
1	Kenderapada	Gyanaranjan Sethi	disc.kendrapara@gmail.com	9853445187
2	Keonjhar	Valentina Pothal	disckeonjhar@gmail.com	9437337124
3	Mayurbhanj	Sebati Kar	disc.mayurbhanj@gmail.com	9438383601
4	Ganjam	A.Guruprasad Dora	disc.ganjam@gmail.com	9692056661
5	Malkanagiri	Subhashish Patnaik	disc.malkangiri@gmail.com	9437915432
6	Khurda	Manas Mohan Brahma	disc.khurda@gmail.com	9778606200
7	Gajapati	K.Chiranjeevi Dora	gajapati.disc99@gmail.com	9692784650
8	Rayagada	Bijaya Kumar Panigrahi	disc.rayagada@gmail.com	9937207819
9	Baragarh	Mastaram Chhanda	disc.bargarh@gmail.com	9438867614
10	Dhenkanl	Nachiketa Sahu	disc.dhenkanal@gmail.com	9438100181
11	Cuttack	Kishore Achary	disc.cuttack@gmail.com	9437285568
12	Nabrangpur	Sobhagyaranjan Nayak	degsnabarangpur@gmail.com	9853102525
13	Sambalpur	Nitesh Ku Khatry	disc1sambalpur@gmail.com	9437401915
14	Deogarh	Bikash Ku Sahu	disc.debagada@gmail.com	9438182223
15	Puri	Piyush Chakravarty	disc.puri@gmail.com	9438285609

16	Nayagarh	Nihar Ranjan Nayak	disc.nayagarh@gmail.com	9861105050
17	Angul	Debadatta Sahu	debadatta.mca@gmail	9778569960
18	Jagatsingpur	Aurobinda Acharya	discjagatsinghpur@gmail.com	9861378581
19	Sonepur	Gupteswar Rana	disc.subarnapur@gmail.com	9778091988
20	Kalahandi	Sanjib Kumar Choudhry	disc.kalahandi@gmail.com	9777045712
21	Bhadrak	Bijayananada Kar	disc.bhadrak@gmail.com	9438412507
22	Jajpur	Sarada Prasad Jena	saradaprasadjena@gmail.com	9937833170
23	Kandhmal	Retashree Barik	disc.kandhamal@gmail.com	9439521304
24	Nuapada	Birendra Singh Dandasena	disc.nuapada@gmail.com	9437950330
25	Sundergargh	Ansuman Purohit	Sundargarh.disc@gmail.com	9937511136
26	Jharsuguda	Sunita Patel	disc.jharsuguda@gmail.com	9937681560
27	Bolangir	Aryanandan Gopalakrishna Sahu	discbolangir@gmail.com	8895252539
28	Koraput	Manoj Kumar Das	degs.koraput@gmail.com	9438479585
29	Boudh	Samir kumar Nayak	degs.boudh@gmail.com	9778321840
30	Balasore	Falguni Dutta	degm.bls@gmail.com	9040271574

5.4 Details of Human Resources trained on Disaster Management

Sl No.	Staff Category	Total staff	No of trained personnel			
			Basic	ToTs	MoTs	Total
1	Administrative	15	Nil	Nil	Nil	Nil
2	Clerical & Financial	10	Nil	Nil	Nil	Nil
3	Project/scheme	32	Nil	Nil	Nil	Nil
4	Menial/Support	11	Nil	Nil	Nil	Nil
Total		68	Nil	Nil	Nil	Nil

5.5 Resource

Sl No	Type of Resource	Description (utility during Disaster & for preparedness)	Details	
			Name of the District/Division	Total (In Nos.)
1	**Infrastructure**			
a				
b				
2	**Support Equipment for DM**			
a				
b				
3	**Human Resources**			
a	Trained on DM			
b	Untrained			
4	**Others (Specify)**			
a				
b				

5.6 Important Contact Nos.

Sl No.	Name of the Agency/Department	Name of the Nodal Person	Contact details

5.7 Preparedness at Department level **(List is Indicative & may be extended)**

- Ensure regular preparedness meetings (preferably quarterly)
- Develop & update Disaster Management Plan, carry out Hazard analysis
- Keep a list of Contacts of EoCs, Nodal officer of different departments, Important stake holders,
- Keep a list of infrastructure/equipment with Operation & Maintenance calendar
- Carry out operation & maintenance of infrastructure / equipment as per schedule
- Develop yearly capacity building calendar of stakeholders & volunteers
- Asses preparedness through Mock Drills for different disasters at district department, block & community level
- Adopt sustainable prevention & mitigation measures
- Integrate DM, DRR & CCA features in development programmes

Chapter -6: Response Plan and Relief

6.1 Public Warning System

6.1.1 Existing arrangements of the department for information collection and dissemination

Helpdesk Team was present around the clock to inform and for receiving response from departments. Also, each members of OSDC and OSWAN are available for receiving any form of information related to any incidents (specific to disaster).

6.1.2 Existing system of Public Warning in the departments.

OSDC has his own installed Public Warning System limited to OSDC Premises only to inform the users of OSDC.

6.1.3 Establishment of control rooms at State and District level

Sl No.	State/Districts	Contact Person	Contact no. of the control room	E-mail ID

6.2 Inter-Departmental Coordination

6.2.1 State Level

6.2.2 District Level

6.2.3 Appointment of Nodal Officers to support Inter-departmental coordination

Sl No.	Level	Name of the Nodal Officer	Contact No.	Alternative contact no.	Roles/Responsibilities
1	Joint Secretary	Aditya Mohapatra	9437168606	0674-2567838	Inter-departmental Co-ordination

6.3 Incident Response Teams (IRTs)

Sl No.	Level	Head of the IRT	Team members	Roles / Responsibilities
1	State	Data Centre Project Manager	1. Member of OSDC Composite Team 2. Members of DCO	1. Coordinate with State Government and other line Departments. 2. Ensure Reporting of the affected area and assess damage thereof. 3. Plan and arrange

				necessary inputs for response measures 4. Maintain an inventory of all related guidelines, procedures, action plans, district maps and Contact numbers. 5. Document the lessons learnt. Circulate printing material on Contingent and DM Plans. 6. Capacity Building

6.4 Disaster Specific Response Plan of the Department

The Disaster Management Strategies to be adopted by the Department is different for each kind of Disaster. Below are the descriptions of such Strategies:

Scenario	Description
Scenario-I (S1)	**Operating from Primary site using DR infrastructure (No people movement)** This strategy will be applicable when critical systems are unavailable at the Data Centre. However the Primary site is accessible and connectivity to the DR site is available. In such cases, the employees can remotely access and start the systems at DR site. It involve some level of coordination between the personnel at the Primary and DR site. However, it must be ensured that critical data needed for Recovery is available at the DR site before system start up.
Scenario- 2 (S2)	**Operating from DR site using the DR infrastructure** This strategy shall be used in case of a disaster that results in unavailability of the city hosting the Primary site *(i.e.* the premises, technology and infrastructure in the city hosting the Primary site are either unavailable or inaccessible). City wide disasters, terrorist attacks, etc. are some of the events that may result in such a failure scenario.

Sl No.	Natural Calamity	Responsibility	Response Time line	Who is responsible
1	Network Penetration / Hacking (Internal/ External)	S1	N/A	Manager – OSDC Composite Team
2	Denial of Service	S1	N/A	do
3	Virus Attack / Malicious Codes / Spam	S1	N/A	do
4	Lightning / Storms	S2	N/A	do
5	Theft / Unavailability of components	S1	N/A	do
6	Air-conditioning failure	S1	N/A	do
7	Power Outage	S2	N/A	do
8	Earthquake	S2	N/A	do
9	Fire	S2	N/A	do
10	Flood	S2	N/A	do

6.5 Roles of NGOs and Voluntary Organization for better coordination

N/A

6.6. Standard Operating procedure for different departments (The list is Indicative & may be extended as per need & requirement)

Name of the Department	On Receiving Warning	Response time	Post Disaster
Electronics & Information Technology	✓ Disseminate the alert to all concerned (Staff list) ✓ Uploading of various information in the state portal ✓ Video conferencing	✓ OSDC ✓ OSWAN ✓ SEC-LAN	✓ Video conferencing facility ✓ Network infrastructure support

6.7 Relief

6.7.1 Reporting Procedures and formats for damage assessment and others

N/A

6.7.2 Illustrative list of activities identified as of an immediate nature

N/A

6.7.3 Minimum Standards of Relief

N/A

6.7.4 Management of relief supplies/speedy management

N/A

Chapter – 7 Restoration & Rehabilitation

Rehabilitation and restoration comes immediately after relief and rescue operation of the disaster. This post disaster phase continues until the life of the affected people comes to normal. This phase mainly covers damage assessment, disposal of debris, disbursement of assistance for houses, formulation of assistance packages, monitoring and review, cases of non-starters, rejected cases, non-occupancy of houses, relocation, town planning and development plans, awareness and capacity building, housing insurance, grievance redress and social rehabilitation etc.

The district is the primary level to respond to any natural calamity & take up restoration & rehabilitation activities wherein the role of the heads of the department play a vital role to evaluate, asses the quantum of loss & report the situation to the Special Relief commissioner/ State Government for assistance. Further, The Department must undertake all the steps for restoration & rehabilitation of all such infrastructure damaged in disaster by supplying essential commodities, group assistance to the affected people, damage assessment and administrating appropriate rehabilitation and restoration measures.

However, for any assistance from the state government the requisition must reach the SDMA & SRC office in the prescribed format as detailed below for smooth & quick processing.

The Damage Assessment Team shall comprise of management, and technical experts who shall assess & report the damage at SDC, and take steps to minimize the extent of the same.

Damage Assessment Team (DAT)	Project Manager – CT DCO Project Manager CT member/s DCO Domain Experts User Department Technical Resources External Vendor Resources

Chapter 8: Recovery:

A series of long term activities framed to improve upon the repaired activities in the Reconstruction & rehabilitation phase are covered under Recovery phase. Recovery includes all aspects of mitigation and also incorporates the continuation of the enabling process, which assists the affected persons and their families not only to overcome their losses, but also to achieve a proper and effective way to continue various functions of their lives. The Recovery process is therefore a long-terms process in which everyone has a role – the Government including the PRI members, NGOs and especially the affected people, their families and the community.

The Role of the Departments are to explore the scope for

- Preparation of Recovery plan for displaced population, vulnerable groups, environment, livelihoods
- Organise initial and subsequent technical assessments of disaster affected areas and determine the extent of recovery works necessitated in addition to reconstruction & rehabilitation works.
- Evaluate the extent of works under SDRF/NDRF & other sources(damaged infrastructures)
- Explore opportunities for external aids like (International Agencies / Civil Society / Corporate Sector)
- Allocate funds for the stabilisation of the repaired & reconstructed infrastructure.
- Integrate Climate change & Disaster Risk Reduction features in the recovery programmes

The heads of the department will be the co-ordinator of all Recovery activities under the department. The role of the Heads of the department will be to:

- Generally monitor the management of the recovery process;
- Ensure implementation of the recovery plan at the district level & below.
- Ensure Effective service delivery minimising overlap and duplication;

The Operations Recovery Team shall comprise of management and technical experts who shall undertake the recovery operations for SDC at the designated DR Site.

Damage Assessment Team (DAT)	Project Manager – CT DCO Project Manager CT member/s

	DCO Domain Experts User Department Technical Resources External Vendor Resources

Chapter – 09:

Mainstreaming Disaster Risk Reduction (DRR) in developmental projects of the department

9.1 Identification of existing programmes of the Department

9.2 Devising plans for factoring Disaster Risk Reduction features into developmental programmes.

[Devise appropriate policy for "Sustainable development" by factoring disaster risk concerns, can help reduce disaster losses, protect existing development gains and avoid new risks. Identify national and other development programs connected with your department and induce strategic interventions for accomplishing "sustainable development" objectives.]

Mainstreaming DRR involves incorporating disaster risk reduction into development policy and practice. It means radically expanding and enhancing disaster risk reduction so that it becomes normal practice, fully institutionalised within an agency's relief and development agenda.

Mainstreaming has three purposes:

(a) To make certain that all the development programmes and projects, are designed with evident consideration for potential disaster risks and to resist hazard impact,

(b) To make certain that all the development programmes and projects do not inadvertently increase vulnerability to disaster in all sectors: social, physical, economic and environment

(c) To make certain that all the disaster relief and rehabilitation programmes and projects are designed to contribute to developmental aims and to reduce future disaster risk.

Mainstreaming DRR into the developmental plans is an important mandate of the Disaster Management Act 2005. Integration of disaster risk reduction measures into ongoing flagship programmes of the department is being used as an entry point for mainstreaming DRR in development plans. Steps for ensuring the incorporation of DRR into various ongoing programmes\plans are as follows:

(a) Identification of key programme /projects of the department.

(b) Identification of entry points within the programme for integration of DRR (structural, nonstructural and other mitigation measures) at various levels viz. state, district and local levels

(c) Close coordination with concerned departments such as State Planning Commission and Finance Department for promoting DRR measures into development plans and policies

(d) Allocation of dedicated budget for DRR within the departmental plans

(e) Preparation of guidelines for integration of disaster risk reduction measures into development plans of the department at the district and sub-district level.

(f) Review & Incorporation of DRR provisions in the policies, rules & regulations

Scope for integrating different schemes for Disaster Risk Reduction (DRR) activities:

Sl. No.	Scheme/ Project	Possible activities for DRR
1.	SDC	
2.	SWAN	
3.	SEC-LAN	

Chapter -10: Provisions for financing the activities

As per the sub-section (2) of Section (40) of the DM act, every department of the state government while preparing the Departmental Disaster Management Plans shall make provision for financing the activities specified therein.

10.1 State Disaster Response Fund (SDRF)

As per the provisions of Disaster Management Act, 2005 sub-section (1)(a) of Section (48) and based on the recommendation of the 13th Finance Commission, the Government of Odisha has constituted the State Disaster Response Fund (SDRF) replacing the Calamity Relief Fund (CRF). The amount of corpus of the SDRF determined by the 13th Finance Commission for each year the Finance Commission period 2010-15 has been approved by the Central Government. The Central Government contributes 75% of the said fund. The balance 25% matching share of contribution is given by the State Government. The share of the Central Government in SDRF is released to the State in 2 installments in June and December respectively in each financial year. Likewise, the State Government transfers its contribution of 25% to the SDRF in two installments in June and December of the same year.

As per the Guidelines on Constitution and Administration of the State Disaster Response Fund (SDRF) laid down by the Ministry of Home Affairs, Government of India, the SDRF shall be used only for meeting the expenditure for providing immediate relief to the victims of cyclone, drought, earthquake, fire, flood, tsunami, hailstorm, landslide, avalanche, cloud burst and pest attack. The State Executive Committee (SEC) headed by the Chief Secretary, SEC decides on all matters connected with the financing of the relief expenditure of immediate nature from SDRF.

(The reporting formats of the department for SDRF norms is annexed at Annexure- 1 to 3)

10.2 National Disaster Mitigation Fund

As per Section 47 of the DM Act 2005, Central Government may constitute a National Disaster Mitigation Fund for projects exclusively for the purpose of mitigation. This Section has not been notified by the Government so far. As mentioned earlier, the FC-XIV restricted its recommendation to existing arrangements on the financing of the already constituted funds (National Disaster Response Fund and State Disaster Response Fund) only, as per its terms of reference. The FC-XIV did not make any specific recommendation for a mitigation fund.

10.3 Recommendations of the Fourteenth Finance Commission

In regard to grants for disaster management, Fourteenth Finance Commission (FC-XIV) has adopted the procedure of the XIII FC and used past expenditures on disaster relief to determine the State Disaster Response Fund corpus. While making recommendations, XIV FC have taken note of the additional responsibility cast on States and their district administrations under the Disaster Management Act. XIV FC has also taken note of the location-specific natural disasters not mentioned in the notified list, which are unique to some States.

10.4 Release of Funds to Departments and Districts:

Funds required towards pure relief to affected persons / families for natural calamities in shape of emergency assistance, organizing relief camp / free kitchen / cattle camp, agriculture input subsidy and other assistances to affected farmers, ex-gratia as assistance for death cases, grievous injury, house building assistance, assistance to fisherman / fish seed farmers / sericulture farmers, assistance for repair / restoration of dwelling houses damaged due to natural calamities are administered through the respective collectors.

Part funds towards repair / restoration of immediate nature of the damaged public infrastructure are released to the Departments concerned. On receipt of requisition from the Collectors / Departments concerned, funds are released after obtaining approval / sanction of S.E.C. However, funds towards pure relief are released under orders of Special Relief Commissioner / Chief Secretary and the same is placed before the State Executive Committee in its next meeting for approval. To save time, Collectors have been instructed to disburse the ex-gratia assistance from the available cash and record the same on receipt of fund from Special Relief Commissioner.

10.5 Allocation by Ministries and Departments

Section 49 provides for Allocation of funds by Ministries and Departments. It states that:

"(1) Every Ministry or Department of the Government of India shall make provisions, in its annual budget, for funds for the purposes of carrying out the activities and programmes set out in its disaster management plan.

(2) The provisions of sub-section (1) shall, *mutatis mutandis*, apply to departments of the Government of the State."

10.6 Fund provision for disaster preparedness & capacity building of the department

(Note: Provision of funds for different capacity building programmes and preparedness measures to be elaborated)

Formats for provision of funds for disaster management in the annual budget of the department

Sl No.	Categories	Sub-Categories	Total provision of funds in lakhs for the financial year 2019-20
1	Mitigation	Structural	2
		Non-Structural	3
2	Capacity-Building	Training Programmes	7
		Mock drills	2
		IEC materials	1
3	Procurement	Materials	2
		Resources	3

10.6 Flexi Funds as a part of Centrally Sponsored Schemes

As per Department of Expenditure, Ministry of Finance, O.M No. 55(5)/PF-II/2011 dated 6.1.14, all Central Ministries shall keep at least 10 percent of their Plan budget for each CSS as flexi-fund (except for schemes which emanate from a legislation or schemes where the whole or a substantial proportion of the budgetary allocation is flexible. States may use the flexi-funds for the CSS to meet the following objectives:

a) Provide flexibility to States to meet local needs and requirements within the overall objective of each program or scheme;

b) Pilot innovations and improve efficiency within the overall objective of the scheme and its expected outcomes;

c) Undertake mitigation /restoration activities in case of natural calamities in the sector covered by the CSS;

The utilization of flexi-funds for mitigation/restoration activities in the event of natural calamity must be in accordance with the broad objectives of the CSS. It is possible to combine flexi-fund component across schemes within the same sector but the flexi-funds of a

CSS in a particular sector however, shall not be diverted to fund activities/schemes in another sector. The flexi-funds constitute a source of funding for mitigation activities within overall objectives of the particular National Disaster Management Plan 143 CSS(s) under which they are allocated and this would still leave a gap in terms of funding purely mitigation related projects especially those addressing cross cutting themes that cover multiple sectors.

(The guidelines of Flexi-funds within centrally sponsored schemes is annexed at Annexure-4)

Annexure- 1

Reporting formats of the department for SDRF norms

Sector	**Damage in Physical terms**	**Requirement of funds for repair of immediate nature**	**Out of (3) amount available from annual budget**	**Out of (3) amount available from related schemes/ programmes / other sources**	**Out of (3) amount proposed* to be met from SDRF/NDRF as per the list of works indicated in the revised items & norms**
1	**2**	**3**	**4**	**5**	**6**
Roads & Bridges					
Drinking water Supply works (Rural)					
Drinking water Supply works (Urban)					
Irrigation					
**Power					
Primary Health Centres					
Community assets in social sectors covered by Panchayats					

Annexure-2

Format for working out the requirements under the head of repair of damaged infrastructure of immediate nature

Sector		Damage in physical terms	Requirement of funds for repair of immediate nature	Out of (3), amount available from annual maintenance budget	Out of (3), amount available from related schemes/ programs/ other sources	Out of (3), amount proposed to be met from CRF/NCCF in accordance with list of works indicated in the Appendix to the revised items and norms
Roads & Bridges	PWD Roads	No. of breaches- Length of Road damaged – No. of culverts damaged – No. of culverts washed away –				
	Rural Roads	No. of Roads damaged – Length of Road damaged – No. of breaches – No. of CD/Bridge damaged– No. of CD/Bridge washed away –				
	Urban Roads	Length of drain damaged – Length of Road damaged No. of culverts damaged –				
	Panchayat Roads	No. of Roads damaged – Length of breaches – Length of Road damaged – No. of culverts damaged – No of culverts washed away				

	River/Canal Embankment Roads	No of Roads damaged in river embankments– Length of Road damaged in river embankments – No of Roads damaged in canal embankments – Length of Road damaged in canal embankments –				
Drinking Water Supply	Rural Water Supply	No of Tube wells damaged – No of platforms damaged – No. of Rural pipe water supply system damaged -				
	Urban Water Supply					
Irrigation	River Embankment	No of breaches – Length of breach in Km – No of partial damage -				
	Canal Embankments	No of breaches – Length of breach in Km – No of partial damage -				
	M I projects	No of Minor Irrigation projects damaged -				
	Clearance of Drainage channels	Length of drainage channels congested with vegetative materials –				
Primary Education	Primary School Buildings	No of Primary School buildings damaged -				
PHCs	PHCs	No of Primary Health Centres damaged -				

Community assets owned by Panchayats	Community Halls	No of Panchayat Ghar/Community Hall damaged -				
	AWW Centres	No of Anganwadi Centres damaged -				
Power	Electrical lines	No of Primary sub-stations damaged – 33 KV lines damaged – 11 KV lines damaged – Distribution Transformers damaged – LT lines damaged –				
		Total				

Annexure-3

Animal Husbandry (Replacement of Animals)

Name of the Block	**No of Livestock / Birds lost**					**No of animals qualifying for relief grant (i.e., subject to ceiling of 3 large Milch animal or 30 small Milch animals or 3 large draught animal or 6 small draught animal per household**				**Expenditure incurred (Milch animals @ Rs.30,000 for large animal , Rs.3000 for small animals & Draught animals @ Rs 25000 for large animal, Rs. 16,000 for small animals)**				**Poultry @ 50/- per bird subject to a ceiling of assistance of Rs.5000/- per beneficiary household.**	**Total expenditure (11+12+13+14 +15)**
	Milch Animal		**Draught Animal**		**Poultry Birds**	**Milch Animal**		**Draught Animal**		**Milch Animal**		**Draught Animal**			
	Buffalo/ Cow	**Sheep / Goat**	**Camel/ Horse/ Bullock**	**Calf/ Donkey / Pony**		**Buffalo/ Cow**	**Sheep/ Goat**	**Camel / Horse/ Bullock**	**Calf/ Donkey/ Pony**	**Buffalo/ Cow**	**Sheep/ Goat**	**Camel / Horse/ Bullock**	**Calf/ Donkey/ Pony**		
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)

Annexure-4

Guidelines of Flexi-funds within Centrally Sponsored Scheme

F.No.55(5)/PF.II/2011
Ministry of Finance
Department of Expenditure
Plan Finance-II Division
*****

New Delhi, dated January 6, 2014

Office Memorandum

Subject: Guidelines for Flexi-Funds within Centrally Sponsored Schemes (CSSs).

Objectives

The introduction of a flexi-fund component within the Centrally Sponsored Schemes (CSS) has been made to achieve the following objectives:-

(i) To provide flexibility to States to meet local needs and requirements within the overall objective of each programme or scheme;
(ii) To pilot innovations and improve efficiency within the overall objective of the scheme and its expected outcomes;
(iii) To undertake mitigation/restoration activities in case of natural calamities in the sector covered by the CSS.

Budgetary Allocation

2. Central Ministries concerned shall keep at least 10% of their Plan budget for each CSS as flexi-funds, except for Schemes which emanate from a legislation (e.g. MGNREGA), or, schemes where the whole or a substantial proportion of the budgetary allocation is flexible (e.g. RKVY)

Allocation of State Share

3. After approval of the Plan Budget, Central Ministries shall communicate tentative allocations for each CSS to States including the allocation of flexi-funds by the end of May of every financial year. In the CSS that are demand-driven or project-driven and it is not feasible to make allocations to States, tentative allocations for a quarter/half-year/year shall invariably be communicated to sates by the end of May of every financial year. Allocation to the States shall be based on transparent and equitable criteria. Central Ministries shall make allocations for 10% of flexi-funds for the CSS amongst States in the same proportion as tentative State allocations in the 90% portion of the CSS.

4. Flexi-funds will be a part of the CSS and the name of the concerned CSS will precede the word 'flexi-funds', in the communication to States. There will be no separate budget and account head for this purpose.

5. As flexi-funds are a part of the concerned CSS, the same State share (including beneficiary contribution, if any) would be applicable for the flexi-fund component as well. However, States may provide additional share (including beneficiary contribution, if any) over and above the required State share for the flexi-funds component of the allocation for the CSS.

Use of flexi-funds

6. States may use the flexi-funds for the CSS to meet the objectives mentioned above in accordance with the broad objectives of the main Scheme. The flexi-funds may also be utilized for mitigation/restoration activities in the event of natural calamities in accordance with the broad objectives of the CSS. However, the specific guidelines of the CSS, applicable for 90% of the CSS allocation, will not be essential for the Flexi-funds component of the CSS, except for State share requirements.

7. The flexi-funds of a CSS in a particular sector, however, shall not be diverted to fund activities/schemes in other sectors. For example, if a particular CSS relates to elementary education, the flexi-funds for that scheme can only be used for elementary education and not for agriculture or any other sector. But it would be permissible to converge flexi-funds of different schemes to improve efficiency and effectiveness of outcomes.

8. The purpose of providing flexi-funds is to enable Sates to undertake new innovative schemes in the particular area covered by the CSS. Flexi-funds shall not be used to substitute State's own non-Plan or Plan schemes/expenditure. It shall also not be used for construction/repairs of offices/residences for Government officials, general publicity, purchase of vehicles/furniture for offices, distribution of consumer durables/non-durables, incentives/rewards for staff and other unproductive expenditure.

9. Schemes taken up with Flexi-funds shall invariably carry the name of concerned CSS.

10. The State-level Sanctioning Committee (SLSC) may sanction projects under the flexi-funds component. States will be not be required to send the project to Ministries for approval under the flexi-funds window as the SLSC will have a representative of the concerned Ministry and Planning Commission.

States wishing to use flexi funds as part of the normal 90% component are free to do so.

Release of Flexi-funds

11. Release of flexi-funds for each CSS may be made on a prorata basis along with the normal releases under CSS. In other words, no separate system for release or for utilization certificates for flexi-funds would be required.

12. Flexi-funds within each CSS will be subject to the same audit requirements as the main CSS including the audit by the Comptroller & Auditor General of India (CAG).

Monitoring & Evaluation

13. Web-based requirements for reporting the use of flexi-funds may be designed by adding modules to the existing MIS. Outcomes (medium term) and outputs (short term) need to be part of the MIS along with pictures/images and good practices to ensure greater transparency and cross-learning across States. For this purpose, web portal for sharing best practices is proposed to be created in Planning Commission.

14. Evaluation of flexi-funds may be done through the existing evaluation processes including those by Ministries, Programme Evaluation Organisation (PEO) and Independent Evaluation Organisation (IEO), Planning Commission and by independent third parties. Terms and conditions for evaluation may be designed in such a manner that outcomes of the Scheme as a whole as well as flexi-funds are well identified/measured.

15. These guidelines will be applicable from the financial year 2014-15.

Saurabh Garg 6/1/14

(Dr. Saurabh Garg)
Joint Secretary (Plan Finance-II)
Government of India

To,

1. Secretaries,
   All the Departments/Ministries
   Government of India.

2. Chief Secretaries,
   All States/Union Territories.

Chapter – 11: Knowledge Management

Knowledge management (KM) is a multidisciplinary approach to achieve the departmental objectives by creating, sharing, using and managing information as well as technology of an organization. Thrust must be given towards exploring all possible opportunities of knowledge requirement for augmenting the departmental potentials like physical assets, human resources & services. Implementing a complete knowledge management takes time and money. However, risks can be minimized by taking a phased approach that gives beneficial returns at each step & tangible results quickly with enhanced efficiency, better decision making and greater use of tested solutions across the department.

Objectives for knowledge Management: Describe the Department Specific objective both short term & long term *(Information & Technology needs and the drivers as well as collaboration that will provide momentum and justification to the endeavor.)*

11.1 Best Practices & innovation in the Department

Thematic Area	Best Practice	Technology Intervention	Opportunity for replication
Cyber Security	Formation of CERT-O	N/A	N/A

11.2 Process for Knowledge management

Technology Needs	Current State of Technology	Prioritization	Collaborating Institute (Address Contact person & details)

11.3 Knowledge partners

Details of Institutions With Address, Mail ID, Contact of Nodal Person			
District Level	**State Level**	**Nation Level**	**International**

Implementation Roadmap for Knowledge Management

Annexure:

- Emergency contact Nos.

Sl. No.	Name	Team Members	Office STD code (0674)	Mobile
1	Shri R.N. Palai	Spl. Secretary, E&IT Department	2567151	9437045200
2	Shri Aditya Mohapatra	Joint Secretary, E&IT Department	2567838	9437168606
3	Smt Madhumita Rath	General Manager, OCAC	2567064	9438295525
4	Shri A.K. Hota	Dy. General Manager (I/C), OCAC	2567295	9437633654
5	Shri S.K.Bhol	Project Manager, OSDC	2567995	9938478383
6	Shri Arun Bairiganjan	System Administrator, OCAC	2567280	9937312169
7	Shri Subrat Mohanty	Sr. Software Engineer, OCAC	2567064	9437233907
8	Shri Satikanta Dash	Consultant, SeMT	2567064	9937585011

- List of Item wise suppliers for department in case of emergency.
- Resource list (IDRN)
- List of NGOs, CBOs, VOs, associated with the department.
- Essential formats for requisition, damage assessment & reporting
- List of infrastructures available with the deptt.
- Reporting formats of the department for SDRF norms
- Format for working out the requirements under the head of repair of damaged infrastructure of immediate nature
- Guidelines of Flexi-funds within Centrally Sponsored Schemes