

Sundernagar Lake



# BHAKRA BEAS MANAGEMENT BOARD INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL

IS/ISO/IEC 27001:2013

**CONTROLLED COPY**

Plot No.6-B/C, Sector-19 B,  
Madhya Marg, Chandigarh-160019  
Phone: +91-172-5011773  
Website: [www.bbmb.gov.in](http://www.bbmb.gov.in)



**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**



**BHAKRA BEAS MANAGEMENT BOARD**

An ISO 9001, 14001 Certified Board

**INFORMATION SECURITY MANAGEMENT SYSTEMS  
MANUAL**

IS/ISO/IEC 27001:2013

**INFORMATION TECHNOLOGY — SECURITY TECHNIQUES —  
INFORMATION SECURITY MANAGEMENT SYSTEMS — REQUIREMENTS**

**COPY NO: - 01**

**ISSUE NO: - 01**

**DATE OF ISSUE: - 23/06/2023**

**REVISION NO: - 00**

**ISSUED TO: -**

Plot No. 6-B/C, Sector-19 B,  
Madhya Marg, Chandigarh- 160019  
Phone : +91- 172-5011773  
Website: [www.bbmb.gov.in](http://www.bbmb.gov.in)



## Section 1- Documented Information

<b>Document Title</b>	Information Security Management Systems Manual- BBMB
<b>Document Number</b>	ISMS/M/01
<b>Document Revision no.</b>	00
<b>Document Issue no.</b>	01
<b>Released Date</b>	23.6.2023
<b>Document Owner</b>	Central Management Representative (CMR) Chief Engineer /Transmission System
<b>Controlled Copy No.</b>	Controlled copy not for library
<b>Document Status</b>	<b>ACTIVE</b>
<b>Document Revision Details</b>	Refer to Change History Record
<b>SIGN OFF MATRIX / DOCUMENT APPROVAL</b>	
<b>Prepared By</b>	<b>Name/Designation</b> Er. Gagan Singh, AD/SS&P
<b>Checked By</b>	Er Harkiranjit Kaur, Deputy Director /Transmission
<b>Reviewed By</b>	Er Surjeet Singh, Director/P&D/(Transmission System)
<b>Approved By</b>	Er. Sanjay Srivastva Chairman
<b>Issued By</b>	Er. Vipin Gupta Chief Engineer/ Transmission System

SIGNATURE

Gagan Singh  
AD/SS&P

Harkiranjit Kaur

S. Srivastava  
Chairman

Vipin Gupta



**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

**CONTENT LIST**

SEC NO.	TITLE	CLAUSE REFERENCES	No. of Pages
	<b>Cover Sheet</b>	-	1
	Content list	-	2
0.1	Revision Status Sheet	-	1
0.2	ISMS Manual Distribution List	-	1
0.3	Authorization & Statement of Intent	-	1
0.4	Guide to ISMS Manual	-	2
0.5	Company Profile	-	4
0.6	Scope	1	1
1	Normative Reference	2	1
2	Terms and Definitions	3	1
3	<b>Context of the organization</b>	4	3
4	Understanding organization and its context	4.1	
4.1	Understanding the needs and expectations of interested parties	4.2	
4.2	Determining the scope of the information Security management system	4.3	
4.3	Information security management system	4.4	
4.4	<b>Leadership</b>	5	2
5	Leadership and commitment	5.1	
5.1	Policy	5.2	
5.2	Organizational roles, responsibilities and authorities	5.3	
5.3	<b>Planning</b>	6	3
6	Actions to address risks and opportunities	6.1	
6.1	General	6.1.1	
6.1.1	Information Security risk assessment	6.1.2	
6.1.2	Information Security risk treatment	6.1.3	
6.1.3	Information Security objectives and Planning to achieve them	6.2	



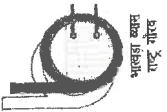
**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

SEC NO.	TITLE	CLAUSE REFERENCES	No. of Pages
7	<b>Support</b>	7	
7.1	Resources	7.1	
7.2	Competence	7.2	
7.3	Awareness	7.3	4
7.4	Communication	7.4	
7.5.1	General	7.5.1	
7.5.2	Creating and updating	7.5.2	
7.5.3	Control of documented information	7.5.3	
8	<b>Operation</b>		1
8.1	Operational planning and control	8.1	
8.2	Information security risk assessment	8.2	
8.3	Information Security risk treatment	8.3	
9	<b>Performance evaluation</b>		3
9.1	Monitoring, measurement, analysis and evaluation	9.1	
9.2	Internal audit	9.2	
9.3	Management review	9.3	
10	<b>Improvement</b>		1
10.1	Nonconformity and corrective action	10.1	
10.2	Continual Improvement	10.2	

SECTION NO.	ISO CLAUSE NO.	TITLE	No. of Pages
1	ANNEXURE "A"	LIST OF PROCEDURES	1
2	ANNEXURE "B"	ISMS POLICY	1
3	ANNEXURE "C"	OBJECTIVES AND TARGET FOR ISMS	1
4	ANNEXURE "D"	PROCESS FLOW CHART, NETWORK DIAGARM	5
5	ANNEXURE "E"	ORGANISATION CHART	4
6	ANNEXURE "F"	ROLE, RESPONSIBILITY & AUTHORITY	36
7	ANNEXURE "G"	Common ISMS Policies & Procedures BBMB	1

Doc.No: ISMS/M/01, Sec no.: 0.1	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 2 of 2
------------------------------------	-----------------	--------------	----------------	-------------

ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN 'PRINTOUT'. LATEST UPDATED COPY IS AVAILABLE WITH MRS AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET

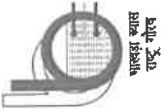


**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

**REVISION STATUS SHEET**

SECTION NUMBER	SHEET NUMBER	REVISION STATUS	REASON FOR REVISION

Doc.No: ISMS/M/01, Sec no.: 0.2	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 1 OF 1
<b>ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WE:LINK AND BBMB INTRANET</b>				



**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

**MANUAL DISTRIBUTION LIST**

<b>SR.NO.</b>	<b>HOLDERS OF CONTROLLED COPY</b>	<b>COPY NO.</b>
01	CE/TS/CMR	01
02	System Software Manager, Chandigarh, MR	02
03	Director Power Regulation BBMB Chandigarh MR	03
04	Director/ P&D(TS), Chandigarh MR	04
05	SE/ Bhakra Powerhouse Circle Nangal MR	05
06	Director/NHP, Chandigarh MR	06
07	Bureau of Indian Standards	07

Doc.No: ISMS/M/01, Sec no.: 0.3	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 1 of 1
<b>ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILAIBLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET</b>				



**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

**AUTHORISATION & STATEMENT OF INTENT**

On behalf of the Management, the Chairman of, BHAKRA BEAS MANAGEMENT BOARD, has assigned the following personnel for the Information Security Management Systems (ISMS) as per requirements of IS/ISO/IEC 27001:2013 standards.

- The Chairman is the Head of the BHAKRA BEAS MANAGEMENT BOARD. He is responsible for ensuring continuing suitability and effectiveness of Integrated Management System as documented in this manual.

- The CMR has assigned the responsibility & authority for implementation, maintenance, and improvement of the Information security Management System.

*राजेश कुमार*

CMR

June, 2023

Doc.No: ISMS/M/01, Sec no.: 0.4	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 1 OF 1
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				





**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

**GUIDE OF ISMS MANUAL**

**1.0 FOREWORD**

This Information security Management Systems (ISMS) Manual describes the Information technology - Security techniques Information security management systems Requirements – adopted by BBMB. This Manual guides the user of the manual through various sections and detailed procedures / documents as relevant.

The ISMS manual has been formulated on the basis of ISO/IEC 27001:2013. This Section titled explains the Structure, Issue and Up-dation procedure of the ISMS Manual. This Manual and the information incorporated herein are the property of BHAKRA BEAS MANAGEMENT BOARD. It must not be reproduced in whole or in part or otherwise disclosed without prior consent in writing from BHAKRA BEAS MANAGEMENT BOARD.

**2.0 STRUCTURE OF THE MANUAL**

This ISMS Manual is structured as shown in the content pages of the Manual. Different sections have been arranged sequentially as per clause number of ISO/IEC 27001:2013. The Manual pages are numbered serially with page number indication. The current revision number and issue number on each page is also indicated. Revision no."00" has been given to first issue of the Section under the issue. This manual is available in English Language only.

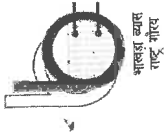
**3.0 MANUAL ISSUE PROCEDURE**

The MR is authorized to carry out the activities of preparing, issuing, maintaining and up-dation of this ISMS Manual.

The distribution of the Manual and the amendment(s) are controlled and MR carries out this activity.

The Master Copy bears the signature of the approving and issuing authority in original. The Master Copy does not bear stamp of "Controlled Copy". The controlled copy of the ISMS Manual is released to all concerned as per the distribution list with red color rubber stamp as "CONTROLLED COPY". Copies of this manual, which are meant for others, are legibly photocopied from Master Copy, and bear no rubber stamp of "CONTROLLED COPY".

Doc.No: ISMS/M/01, Sec no.: 0.5	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 1 OF 2
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				



## INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL IS/ISO/IEC 27001:2013

Additional copies of the Manual, required by external agencies if any, are issued by MR and such copies of the Manual are stamped with red color rubber stamp as "UNCONTROLLED COPY". These uncontrolled copies do not come under the purview of document amendment procedure and are not used within the BHAKRA BEAS MANAGEMENT BOARD, CHANDIGARH.

### 4.0 MANUAL REVISION AND UPDATION PROCEDURE

The ISMS Manual is reviewed periodically by the MR and concerned departments. No revision is implemented unless it has been approved and formally issued.

Each revision is introduced formally, by the MR by updating the manual for use of the personnel identified in the distribution list.

When revisions take place, the revisions are indicated by the revision number in each of the revised sections and are recorded in the Revision Status Sheet.

### 5.0 DOCUMENT NUMBERING SYSTEM:

The documents are coded uniquely for identification purpose.

### 6.0 ORIGINAL

Original Document is the one which is duly endorsed (signed) and authorized for use. The original Document will be used for generating "CONTROLLED COPY" and "UNCONTROLLED COPY", as required.

### 7.0 CONTROLLED COPY

Copy of the original is replaced with the updated version of the same after any revision / change is made to "ORIGINAL".

### 8.0 UNCONTROLLED COPY

The copy of the original which is not updated.

Doc.No: ISMS/M/01, Sec no.: 0.5	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 2 of 2
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				



## COMPANY PROFILE

### PROFILE OF THE ORGANIZATION (BBMB)

#### 1. Bhakra Beas Management Board (BBMB)

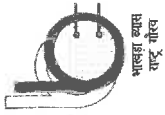
Bhakra-Nangal Project was taken up as a joint venture of states of erstwhile Punjab and Rajasthan. On re-organization of erstwhile Punjab State in 1966, 'Bhakra Management Board' was constituted on 1st October 1967 under Section 79 of Punjab Re-organization Act, 1966 for administration, maintenance, and operation of Bhakra-Nangal Project. Beas Construction Board was constituted under the Punjab Re-organization Act, 1966 for construction of Beas -Project. 'Bhakra Management Board' was renamed as 'Bhakra Beas Management Board' (BBMB) w.e.f. 15th May 1976 after transfer of Beas Project on its completion by Beas Construction Board.

#### 2. Substation Automation System (SAS) and Remote-control Centre for BBMB Barnala & Sangrur substation

SAS and RCC for 220kVsubstation Barnala and Sangrur has been set up as first state of the art project for automation system for control, monitoring, measurement protection metering and communication function of 220kV BBMB Barnala S/stn. Its remote-control Centre has been set up at 220KV Sub Station Sangrur. This SAS system will also be provided at 220 kV S/stn Samaypur, Ballabhgarh, Hisar and Charkhi Dadri in near future with RCC at Bhiwani and Chandigarh, which may have interconnection with SCADA at Chandigarh. It has been achieved by retro fitting of the existing equipment with new latest IEC 61850 compliant equipment like new IED's wherever required. It essentially consists of Bay Control Intelligent Electronics Devices for control and monitoring Station Human Machine Interface and DR workstation is provided to enable local station control via PC by means of HMI and control software package (Micro SCADA) by ABB which contain an extensive range of supervisory control and data acquisition (SCADA) functions. The server has been provided in hot and standby mode. DR workstation provided at the local station also perform the function of engineering workstation to achieve the change of Numerical relay setting, formation of PSL, extraction of DRs etc. of the Numerical relay installed on the panels in control room at Barnala substation. The uploading of DRs from numerical IED's to the DR cum Engineering workstation at local remote station is affected automatically.

One No. DR cum Engineering workstation is also provided at Remote Control Centre (RCC) at Sangrur Substation to view event, records, DRs on demand from Barnala over Ethernet using existing FO network and for effecting relay parameterization, PSL etc. Redundant HMI i.e., Operator workstation at RCC Redundant managed switched Ethernet LAN communication

Doc.No: ISMS/M/01, Sec no.: 0.6	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 1 of 4
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				



## INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL IS/ISO/IEC 27001:2013

infrastructure with hot standby has been provided. Gateways for remote control via industrial grade hardware to RCC at Sangrur on IEC 60870-5-104 have been provided. Gateway for communication with Load Dispatch Centre at Chandigarh via industrial grade hardware on IEC 60870-5-104 protocol matching with existing SCADA of M/s Siemens make have been provided. SAS has got redundant Gateways (Hardware as well as software) for communication to RCC & LDC.

BBMB has been promoting the cause of Renovation, Modernization and Up-rating of old Hydro Power Houses in the country. This task has already been undertaken for all the BBMB Power Houses.

### 3.Substation Automation System (SAS)

This system has been set up for automated control, monitoring, metering and protection, operation of different bays of 220kV substation Barnala SAS system on the IEC 61850 protocol and has outside communication through IEC60870-5-104 protocol to Remote Control Centre (RCC) at Sangrur and Chandigarh. RCC at Sangrur is functional and RCC at Chandigarh will be made functional in near future.

**Justification:** As the SAS system has been designed for process control and monitoring at bay level of the substation and is interconnected with SCADA as well as has its own network at station level. Any disruption/ wrong function of bay level process function scan lead to catastrophic damage to the power system.

**Remote Control Centre:** This consists of all the duplicated major communication/IT infrastructure for same function from RCC at Sangrur.

- **Justification:** Any disruption/wrong function of bay level process function from RCC can also lead to major damage to the power system.

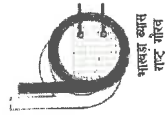
#### Infrastructure

The basic SAS architecture (copy enclosed) which has been implemented at BBMB Substations Barnala and Sangrur mainly consists of the following modules: Local OWS-1 and OWS-2: HMI for local control, monitoring, protection, metering and measurement at Barnala substation. One is in operation and other kept as hot stand by.

#### DR Workstation (Local):

HMI for analysis of disturbance recorder/event records of different IEDs of the Barnala Substation. This is also used for Engineering applications and located at Barnala Substation control room.

Doc.No: ISMS/M/01, Sec no.: 0.6	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 2 of 4
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRS AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				



**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

**VMS:**

This is for PTZ cameras installed at different location at 220KV substation Barnala for visual monitoring of substation infrastructures. Remote OWS-1 and OWS-2: HMI for remote control, monitoring, protection, metering and measurement functions at Sangrur substation. DR workstation

**(Remote):**

HMI for analysis of disturbance record/event records of different IED's installed at Barnala substation. This workstation is also used for Engineering applications by Engineer at remote end i.e. at Sangrur Substation. Micro SCADA Gateway-I: This Gateway is being used for SCADA application for communication at remote end Sangrur Substation / Chandigarh SLDC/RCC. Micro SCADA Server- I: This is the main server for substation automation system at Barnala Substation. Micro SCADA Gateway-II: This "Gateway will be used for SCADA application for communication at remote end at Sangrur/Chandigarh SLDC/RCC. Micro SCADA Server- II: This is the standby server for substation automation system at Barnala Substation

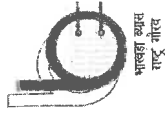
**4. Bhakra Beas Management Board (BBMB) SLDC COMPLEX**

The System Load Dispatch Centre (SLDC) of Bhakra Beas Management Board is assigned with the responsibility of Round the Clock Monitoring, Operation and Control of BBMB Transmission and Generation Assets. BBMB SLDC is equipped with State of Art Supervisory Control & Data Acquisition and Energy Management System (SCADA/EMS) and a dedicated Optical Fiber based Communication System which helps the SLDC Engineers in discharging their responsibilities efficiently, by taking informed decisions duly assisted and guided by the latest technologies.

Keeping pace with the technology, the SCADA/EMS System of BBMB SLDC has been recently upgraded. The new system has a host of new features, which provides greater insights into Power System Monitoring and Control. BBMB has also established its backup SLDC by sharing the infrastructure with PSTCL, thereby providing a unique and cost-effective solution to ensure continuity of services in case of any disaster. By sharing the backup of SLDC with PSTCL, BBMB saved about Rs. 5 Crores in the project cost for itself as well as for PSTCL. BBMB has also equipped its 10 important Generating Stations and Sub-Stations with the State of Art RTUs.

The SCADA/EMS equipment installed at BBMB SLDC comprises of various Servers, Data Storage Devices, Firewalls, Video Projection System, Operator Controls, Remote Controls etc. In addition to the above a dedicated web server has been installed at BBMB SLDC. The web server automatically fetches real time data and single line diagrams from SCADA data and download reports pertaining to BBMB Power System. The external users can connect to web servers through Internet to view SLDC data, display & reports.

Doc.No: ISMS/M/01, Sec no.: 0.6	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 3 of 4
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRS AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				



In addition, all BBMB Power Houses and Sub-stations have been provided with dedicated SCADA remote controls. These remote consoles are connected to BBMB SLDC through a dedicated communication link. With the help of these remote consoles the Sub-station/Power houses officers/staff can monitor the status of various power system devices installed in their own Sub-station as well as other Sub-stations of BBMB. In addition to this the reports pertaining to each Power House and Sub-station can be generated by their Control Room Engineers/Staff. Through their concerned efforts, the Engineers at BBMB SLDC have pioneered various innovative techniques in Power System Monitoring, Operation and Control and continue to march forward towards their goal for implementation of Smart Grid in BBMB.

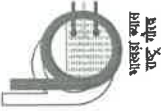
### 5 Bhakra Power Houses

Bhakra Left & Right Bank Power Houses Bhakra Project is a marvel in engineering. The 225.55 m high Dam is of concrete straight gravity type having a gross storage capacity of 9621 million cum. Installed capacity of Bhakra Right Bank Power House is 911 MW (1x126+5x157 MW) and that of Bhakra Left Bank Power House is 504 MW (4x126 MW).

### 6.NHP Project

National Hydrology project is a Central Sector Scheme of Ministry of Water Resources, River Development and Ganga Rejuvenation, GOI The total duration of project is eight years starting from 2016-17 and ending in 2023-24. Bhakra Beas Management Board (BBMB), Chandigarh is one of the implementing agencies of the project (NHP). Bhakra Beas Management Board (BBMB) is one of the eight central agencies, participated in HP-II under the vertical extension component. BBMB has developed a Real Time Decision Support System for Operational Management of BBMB Reservoirs. Bhakra Beas Management Board (BBMB) has set up Earth Receiving Station (ERS) at Chandigarh for inflow forecasting (i.e., short term 3 days and medium term 7 to 15 days) / flood forecasting for optimum utilization of Bhakra and Pong Reservoirs and Canal Network. BBMB has been the 'first mover' in the country. Under this project, 87 no. Real Time Data Acquisition stations comprising Automatic Rain Gauge Stations, Automatic Full Climate Stations, Snow Water Equivalent, Water Level Recorders etc. had been installed in the catchment of River Sutlej and Beas by using state of the art technology. The installations are currently being upgraded through an ongoing contract and an upcoming proposal through which, new stations are also being added. The schematic arrangement of Real Time Decision Support System involves real time transmission of Hydro meteorological data through INSAT-3D at 1 hour interval to Earth Receiving Station at Chandigarh. Real Time Data is processed using Rainfall Runoff Model, Hydro Dynamic Model, Flood Model and Water Allocation of MIKE software. The outcome/ scenario generation is further shared on NHP Dashboard accessible to all.

Doc.No: ISMS/M/01, Sec no.: 0.6	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 4 of 4
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				



# INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL IS/ISO/IEC 27001:2013

## SCOPE

### 1. Scope

This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System within the context of the organization. This International Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this International Standard are generic and are intended to be applicable to

The Scopes of certification for IS/ISO/IEC 27001:2013, which are as follows: -

“Information Technology COMMUNICATIONS SUPPORT SYSTEM In Bhakra Beas Management Board BBMB, Chandigarh, Transmission System, System Operations, 06 Nos. Power Houses, 22 Nos Sub Stations & National Hydrology Project, Chandigarh”.

### Boundary of Scope

BBMB IT-OT systems within the scope consist of:

- a) LAN/WAN System deployed throughout BBMB
- b) SCADA/EMS & URTDSM system at SLDC Complex Chandigarh
- c) Smart Substations (SAS) at Barnala and Sangrur.
- d) SCADA system at Bhakra Left Power house, including remote control at SLDC, Chandigarh
- e) Real Time Decision Support system (RTDSS) under NHP Project, Chandigarh

Doc.No: ISMS/M/01, Sec no.: 1	Revision No: 00	Issue No: .01	Rev. Date: NIL	Page 1 of 1
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRS AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				



**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

**NORMATIVE REFERENCES:**

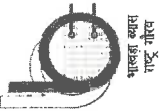
**IS/ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary**

**Statutory & Regulatory Requirements:**

All applicable statutory and legal requirements related to BBMB activities are identified and described in the Legal Register for evaluation

Doc.No: ISMS/M/01, Sec no.: 2	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 1 of 1
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				





**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

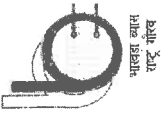
**TERMS & DEFINITIONS**

**3. TERMS & DEFINITIONS**

For the purpose of this document, the terms and definitions given in IS/ISO/IEC 27000 apply

**3.1 Abbreviations:**

Sr. NO.	ABBREVIATION	EXPLANATION
1	BBMB	BHAKRA BEAS MANAGEMENT BOARD
2	CMR	Central Management Representative
3	CE	Chief Engineer
4	TS	Transmission system
5	SAS	Substation Automation system
6	NAS	Network Attached storage
7	PH	Powerhouse
8	MR	Management Representative
9	SCADA	Supervisory control and data acquisition
10	DD	Deputy Director
11	AD	Assistant Director
12	CISO	Chief Information Security Officer
13	AM	Assistant Manager
14	ENGR/PROGRAMMER	ENGINEER/PROGRAMMER
15	AE	Assistant Engineer
16	JE	Junior Engineer
17	EMS	Environment Management System
18	FIN	Finance
19	WI	Work Instructions
20	HOD	Head of the department
21	HR	Human Resource
22	IA	Internal Audit
23	VO	Vigilance Officer
24	IT	Information Technology
25	M&SC	Mechanical and Store Complex
26	Mech.	Mechanical
27	MRM	Management Review Meeting
28	NCR	Non-Conformance Report
29	SStn	Sub Station
30	SR.	Senior
31	OIC	Officer In-Charge
32	PRO	Public Relation Officer
33	QA	Quality Assurance
34	ISMS	Information security Management System



**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

**CONTEXT OF THE ORGANISATION**

**4 Context of the organization**

**4.1 Understanding the organization and its context**

BBMB concerned MR determined external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

External Issues	Internal Issues
MOU Targets	Availability of Generation Unit
Complaints from interested parties	Short fall in IT&C Facilities
Managing contract work force	Availability of Inputs
Legal obligation	Knowledge and skill up gradation
Communication Link Failure	

Monitoring & review of External & Internal Issues:

External Issues	Monitoring, Review & Frequency	Internal Issues	Monitoring, Review & Frequency
MOU	Daily/Monthly	Availability of equipment	Daily
Complaints from interested parties	Mgt. Review Meeting (Once in a year)	Short fall in IT&C Facilities	Daily
Managing contract work force	Terms & condition of contract (Daily)	Availability of water	Daily
Legal obligation	Mgt. Review Meeting	Knowledge and skill upkeep	Training/ communication
Communication Link Failure	As and when required		



**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

**4.2 Understanding the needs and expectations of interested parties**

BBMB, concerned MR determined:

- a) interested parties that are relevant to the information security management system; and
- b) the requirements of these interested parties relevant to information security.

**NEEDS & EXPECTATIONS OF THE INTERESTED PARTIES**

Interested Party	Needs/ Expectations	Monitoring/ Review
Govt. & beneficiaries	Generation as per MOU	Monthly compliance of MOU (Ref: DGR)
Employees	Amenities in workplace	Monthly meeting
	Availability of IT Facilities	concerned MR
	Knowledge/skill enhancement	Training, involvement in improvement activities. Mgt Review meeting
Contractors	Safe working environment	Management/EIC (Ref: as per Contract Agreement)
	Timely Payment	Engineer in Charge to Monitor pending liability
	Availability of Site	Engineer in Charge to Monitor
	Amenities in place	Engineer in Charge to Monitor
Society: Pollution risk /Flood Risk	Compliance to legal norms	Monitor & review as per legal norms



INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013

### 4.3 Determining the scope of the Information Security Management System

BBMB, concerned MR determined the boundaries and applicability of the information security management system to establish its scope.

When determining this scope, BBMB, concerned MR consider:

- a) the external and internal issues referred to in 4.1;
- b) the requirements referred to in 4.2; and
- c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

The scope is available as documented information. The Scope is as below:-

Ref: SECTION NO. ISMS:1

### 4.4 Information Security Management System

BBMB, concerned MR established, implemented, maintained and continually improved an information security management system, in accordance with the requirements of this International Standard.

Ref: SECTION NO: ISMS ANNEX “D”

Doc.No: ISMS/M/01 Sec no : 4	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 3 of 3
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				



**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

## LEADERSHIP

### 5. Leadership

#### 5.1 Leadership and commitment

Top management demonstrated leadership and commitment with respect to the information security management system by:

- a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;
- b) ensuring the integration of the information security management system requirements into the organization's processes;
- c) ensuring that the resources needed for the information security management system are available;
- d) communicating the importance of effective information security management and of conforming to the information security management system requirements;
- e) ensuring that the information security management system achieves its intended outcome(s);
- f) directing and supporting persons to contribute to the effectiveness of the information security management system;
- g) promoting continual improvement; and
- h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

#### 5.2 Ref: Minutes of Meeting of 1<sup>st</sup> MRM, ISMS Policy Annexure B Policy

Top management established an information security policy that:

- a) is appropriate to the purpose of the organization;
- b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;
- c) includes a commitment to satisfy applicable requirements related to information

Doc.No: ISMS/M/01,  
Sec no.: 5

Revision No: 00

Issue No: 01

Rev. Date: NIL

Page 1 of 2

**ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET**



**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

security; and

- d) includes a commitment to continual improvement of the information security management system.

The information security policy :

- e) be available as documented information;
- f) be communicated within the organization; and
- g) be available to interested parties, as appropriate.

**Ref: SECTION NO: ISMS ANNEX “B”, Common ISMS Policies & Procedures (BBMB Chandigarh)**

### **5.3 Organizational roles, responsibilities and authorities**

Top management ensured that the responsibilities and authorities for roles relevant to information security are assigned and communicated.

Top management assigned the responsibility and authority for:

- a) ensuring that the information security management system conforms to the requirements of this International Standard; and
- b) reporting on the performance of the information security management system to top management.

**Ref: SECTION NO: ISMS ANNEX “E” and “F”**

Doc.No: ISMS/M/01, Sec no.: 5	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 2 of 2
<b>ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET</b>				



**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

**PLANNING**

**6. Planning**

**6.1 Actions to address risks and opportunities**

**6.1.1 General**

When planning for the Information Security Management System, BBMB, concerned MR considered the issues referred to in 4.1 and the requirements referred to in 4.2 and determined the risks and opportunities that need to be addressed to:

- a) Ensured the Information Security Management System can achieve its intended outcome(s);
  - b) prevented, or reduced, undesired effects; and
  - c) achieved continual improvement.
- BBMB, concerned MR planned:
- d) actions to address these risks and opportunities; and
  - e) how to
    - 1) integrate and implement the actions into its information security management system processes; and
    - 2) evaluate the effectiveness of these actions.

**Ref: Risk Identification Register (DOC NO: ISMS/RISK/01)**

**6.1.2 Information security risk assessment**

BBMB, concerned MR defined and applied an information security risk assessment process that:

- a) establishes and maintains information security risk criteria that include:
  - 1) the risk acceptance criteria; and
  - 2) criteria for performing information security risk assessments;
- b) ensures that repeated information security risk assessments produce consistent, valid and comparable results

Doc.No: ISMS/M/01, Sec no.: 6	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 1 of 3
<b>ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET</b>				



INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013

- c) identifies the information security risks:
    - 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and
    - 2) identify the risk owners;
  - d) analyses the information security risks:
    - 1) assess the potential consequences that would result if the risks identified in 6.1.2 (c) 1 were to materialize;
    - 2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 (c) 1; and
    - 3) determined the levels of risk;
  - e) evaluates the information security risks:
    - 1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and
    - 2) prioritize the analyzed risks for risk treatment.
- BBMB, concerned MR retained, documented information about the information security risk assessment process.

Ref: Risk Identification Register (DOC NO: ISMS/RISK/01), Risk Assessment Formula, Common ISMS Policies & Procedures (BBMB Chandigarh)/ BBMB/COM/ISM/P/11

**6.1.3 Information security risk treatment**

BBMB, concerned MR defined and applied an information security risk treatment process to:

- a) select appropriate information security risk treatment options, taking account of the risk assessment results;
- b) determined all controls that are necessary to implement the information security risk treatment option(s) chosen;
- c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted

Doc.No: ISMS/M/01, Sec no.: 6	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 2 of 3
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				





**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

- d) produced a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls
- e) formulated an information security risk treatment plan; and obtained risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.

BBMB, concerned MR retained documented information about the information security risk treatment process.

**Ref: Risk Identification Register (DOC NO: ISMS/RISK/01), SOA**

## 6.2 Information security objectives and planning to achieve them

BBMB, concerned MR established information security objectives at relevant functions and levels. The information security objectives:

- a) be consistent with the information security policy;
- b) be measurable (if practicable);
- c) take into account applicable information security requirements, and results from risk assessment and risk treatment;
- d) be communicated; and
- e) be updated as appropriate.

BBMB, concerned MR retained documented information on the information security objectives.

When planning how to achieve its information security objectives, BBMB, concerned MR determined:

- f) what will be done;
- g) what resources will be required;
- h) who will be responsible;
- i) when it will be completed; and
- j) how the results will be evaluated.

**Ref: SECTION NO: ISMS ANNEX "C" and Risk Identification Register (DOC NO: ISMS/RISK/01 )**

Doc.No: ISMS/M/01, Sec no.: 6	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 3 of 3
<b>ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET</b>				



**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

**SUPPORT**

**7.0 Support**

**7.1 Resources**

BBMB, concerned MR determined and provided the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

**7.2 Competence**

The organization:

- a) determined the necessary competence of person(s) doing work under its control that affects its information security performance;
- b) ensured that these persons are competent on the basis of appropriate education, training, or experience;
- c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and
- d) retain appropriate documented information as evidence of competence.

**Ref: Procedure PR: 01**

**7.3 Awareness**

Persons doing work under the BBMB, concerned MR's control aware of:

- a) the information security policy;
- b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and
- c) the implications of not conforming with the information security management system requirements.

**Ref: Procedure PR: 01, Common ISMS Policies & Procedures (BBMB Chandigarh)/BBMB/COM/ISM/P/1-13/ANNEXURE-G**

Doc.No: ISMS/M/01, Sec no.: 7	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 1 of 4
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				



**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

**7.4 Communication**

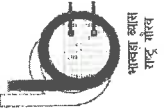
BBMB, concerned MR determined the need for internal and external communications relevant to the information security management system including:

- a) on what to communicate;
- b) when to communicate;
- c) with whom to communicate;
- d) whom to communicate; and
- e) the processes by which communication be effected.

Ref: Procedure PR: 02

**a) Communication Matrix**

Sl. No	Description of Communication	Mode of Communication	Responsibility	Frequency	Communicated To				
					Within Dept	MR	contractors/visitors	Customers	Interested Party
1.	ISMS Policy	Verbal/ Training Displays	HOD	All time	✓ ✓	✓ ✓	✓	✓	✓
2.	ISMS Objectives	Verbal Displays in Department	HOD	Monthly All time	✓ ✓	✓			
3.	Management Programs	Verbal Displays in Department	HOD	Monthly All time	✓ ✓	✓			
4.	Work Instructions	Displays On-Job Training	HOD	All time At least once	✓ ✓		✓		
5	Audit results	Audit Report	MR HOD	Yearly	✓	✓			
6	Corrective Actions	Circulation Of Minutes of meetings	MR HOD	Once in 6 Months	✓ ✓	✓			



**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

Sl. No	Description of Communication	Mode of Communication	Responsibility	Frequency	Communicated To				
					Within Dept	MR	contractors/visitors	Customers	Interested Party
7	ISMS Risks	Doc Verbal On the job training	Concerned HODs	At least once / when there is any change	✓	✓	✓		
8	Applicable Legal Requirements	Legal Register Legal Compliance Report	HOD(HR)	Quarterly As and when	✓		✓		
9	Suggestions	Verbally Management Review Meeting	HODs	As and when required As and when required	✓		✓		
10	ISMS Documentation	On the job Training	HOD – HR	On change of key personnel	✓				

### 7.5 Documented information

#### 7.5.1 General

The BBMB, concerned MR's Information Security Management System includes:

- a) documented information required by this International Standard; and
- b) documented information determined by the BBMB, concerned MR as being necessary for the effectiveness of the information security management system.

Doc.No: ISMS/M/01, Sec no.: 7	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 3 OF 4
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				

**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**



### 7.5.2 Creating and updating

When creating and updating documented information BBMB, concerned MR ensured appropriate:

- a) identification and description (e.g., a title, date, author, or reference number);
- b) format (e.g., language, software version, graphics) and media (e.g., paper, electronic); and
- c) review and approval for suitability and adequacy.

**Ref: Procedure PR: 03**

### 7.5.3 Control of documented information

Documented information required by the information security management system and by this International Standard be controlled to ensure:

- a) it is available and suitable for use, where and when it is needed; and
- b) it is adequately protected (e.g., from loss of confidentiality, improper use, or loss of integrity).  
For the control of documented information, BBMB, concerned MR addresses the following activities, as applicable
  - c) distribution, access, retrieval and use;
  - d) storage and preservation, including the preservation of legibility;
  - e) control of changes (e.g. version control); and
  - f) retention and disposition.

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, be identified as appropriate, and controlled.

**Ref: Procedure PR: 03**

Doc.No: ISMS/M/01, Sec no.: 7	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 4 of 4
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				



## OPERATION

### 8. Operation

#### 8.1 Operational planning and control BBMB

Concerned MR planned, implemented and controlled the processes needed to meet information security requirements, and to implement the actions determined in 6.1. BBMB, concerned MR also implemented plans to achieve information security objectives determined in 6.2.

BBMB, concerned MR kept documented information to the extent necessary to have confidence that the processes have been carried out as planned.

BBMB, concerned MR controlled planned changes and reviewed the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

**BBMB, concerned MR ensured that outsourced processes are determined and controlled**

#### 8.2 Information security risk assessment

BBMB, concerned MR performed information security risk assessments at planned intervals or when significant changes are proposed or occurred, taking into account of the criteria established in 6.1.2 a).

BBMB, concerned MR retained documented information of the results of the information security risk assessments.

**Ref: Risk Identification Register (DOC NO: ISMS/RISK/01 )**

#### 8.3 Information security risk treatment

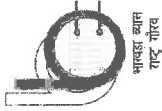
BBMB, concerned MR implemented the information security risk treatment plan.

BBMB, concerned MR documented information of the results of the information security risk treatment.

**Ref: Risk Identification Register (DOC NO: ISMS/RISK/01)**

Doc.No: ISMS/M/01, Sec no.: 8	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 1 of 1
----------------------------------	-----------------	--------------	----------------	-------------

ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET



**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

**PERFORMANCE EVALUATION**

**9. Performance evaluation**

**9.1 Monitoring, measurement, analysis and evaluation**

BBMB, concerned MR evaluated the information security performance and the effectiveness of the information security management system.

BBMB, concerned MR determined:

- a) what needs to be monitored and measured, including information security processes and controls;
- b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;
- c) when the monitoring and measuring be performed;
- d) who monitor and measure;
- e) when the results from monitoring and measurement be analyzed and evaluated; and
- f) who analyze and evaluate these results.

BBMB, concerned MR retained appropriate documented information as evidence of the monitoring and measurement results.

**Ref: Procedure PR: 04**

**9.2 Internal audit**

BBMB, concerned MR conducted internal audits at planned intervals of six months to provide information on whether the Information Security Management System:

- a) conforms to
  - 1) the BBMB, concerned MR's own requirements for its information security management system; and
  - 2) the requirements of this International Standard;
- b) is effectively implemented and maintained

Doc.No: ISMS/M/01, Sec no.: 9	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 1 of 3
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEFLINK AND BBMB INTRANET				



The BBMB, concerned MR:

- c) Planned, established, implemented and maintained an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) taken into consideration the importance of the processes concerned and the results of previous audits;
- d) defined the audit criteria and scope for each audit;
- e) selected auditors and conducted audits that ensured objectivity and the impartiality of the audit process;
- f) ensured that the results of the audits are reported to relevant management; and
- g) retained documented information as evidence of the audit programme(s) and the audit results.

Ref: Procedure PR: 05

### 9.3 Management review

Top management reviewed the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The management review included consideration of:

- a) the status of actions from previous management reviews;
- b) changes in external and internal issues that are relevant to the information security management system;
- c) feedback on the information security performance, including trends in:
  - 1) nonconformities and corrective actions;
  - 2) monitoring and measurement results;
  - 3) audit results; and
  - 4) fulfilment of information security objectives;
- d) feedback from interested parties;
- e) results of risk assessment and status of risk treatment plan; and
- f) opportunities for continual improvement.

Doc.No: ISMS/M/01, Sec no.: 9	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 2 of 3
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				





**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

The outputs of the management review included decisions related to continual improvement opportunities and any needs for changes to the Information Security Management System.

BBMB, concerned MR retained documented information as evidence of the results of management reviews.

**Ref: Procedure PR: 06**

Doc.No: ISMS/M/01, Sec no.: 9	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page <b>3 of 3</b>
<b>ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET</b>				



**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

**IMPROVEMENT**

**10. Improvement**

**10.1 Nonconformity and corrective action**

When a nonconformity occurs, the BBMB, concerned MR

a) reacted to the nonconformity, and as applicable:

- 1) taken action to control and correct it; and
- 2) dealt with the consequences;
- b) evaluated the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:
  - 1) reviewing the nonconformity;
  - 2) determining the causes of the nonconformity; and
  - 3) determining if similar nonconformities exist, or could potentially occur;
- c) implemented any action needed;
- d) reviewed the effectiveness of any corrective action taken; and
- e) made changes to the information security management system, if necessary.

Corrective actions be appropriate to the effects of the nonconformities encountered.

BBMB, concerned MR retained documented information as evidence of:

- f) the nature of the nonconformities and any subsequent actions taken, and
- g) the results of any corrective action.

**Ref: Procedure PR: 07**

**10.2 Continual improvement**

BBMB, concerned MR continually improved the suitability, adequacy and effectiveness of the information security management system.

Doc.No: ISMS/M/01, Sec no.: 10	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 1 of 1
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRS AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				



INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013

CONTROLLED COPY

LIST OF PROCEDURES

PROCEDURE SECTION NO.	TITLE	NO. OF PAGES
PR:01	Competence	1
PR:02	Communication	2
PR:03	Control of documented information	5
PR:04	Analysis and evaluation	1
PR:05	Internal audit	1
PR:06	Management review	2
PR:07	Nonconformity and corrective action	1

Doc.No: ISMS/M/01, Sec no.: Annex-A	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 1 of 1
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				



## ISMS POLICY

### INFORMATION SECURITY MANAGEMENT SYSTEM POLICY

#### OUR AIM

- To establish, maintain and continually improve the performance of our Information Security Management System.

#### OUR COMMITMENTS

- To satisfy applicable requirements related to information Security.
- To continually improve our Information Security Management System by setting objectives and targets

#### OUR ENDEAVOUR

- To motivate employees and associates for the Information Security Management System.

June 2023

*S. Srivastava.*  
Chairman

Doc.No: ISMS/M/01,  
Sec no.: Annex-B

Revision No: 00

Issue No: 01

Rev. Date: NIL

Page 1 OF 1

ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET

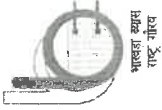


OBJECTIVES & TARGETS FOR THE YEAR 2023-24

SR. NO.	Management System	Objectives	Targets	Responsibility
1	ISMS	Complaints from interested parties	Nil	CONCERNED MR
2	ISMS	Availability of IT Services (Internet-services, mailing services, Web services etc.)	100%	CONCERNED MR
3	ISMS	Availability of IT Facilities (Hardware, equipment, LAN etc.)	100%	CONCERNED MR
4	ISMS	Availability of Internet Lease Line Link, MPLS Link	100%	CONCERNED MR
5	ISMS	Availability of physical media/OFC/ Link within BBMB From data center to various departments.	100%	CONCERNED MR
6	ISMS	Training of Employees/ Contract workers	Once in a year	CONCERNED MR

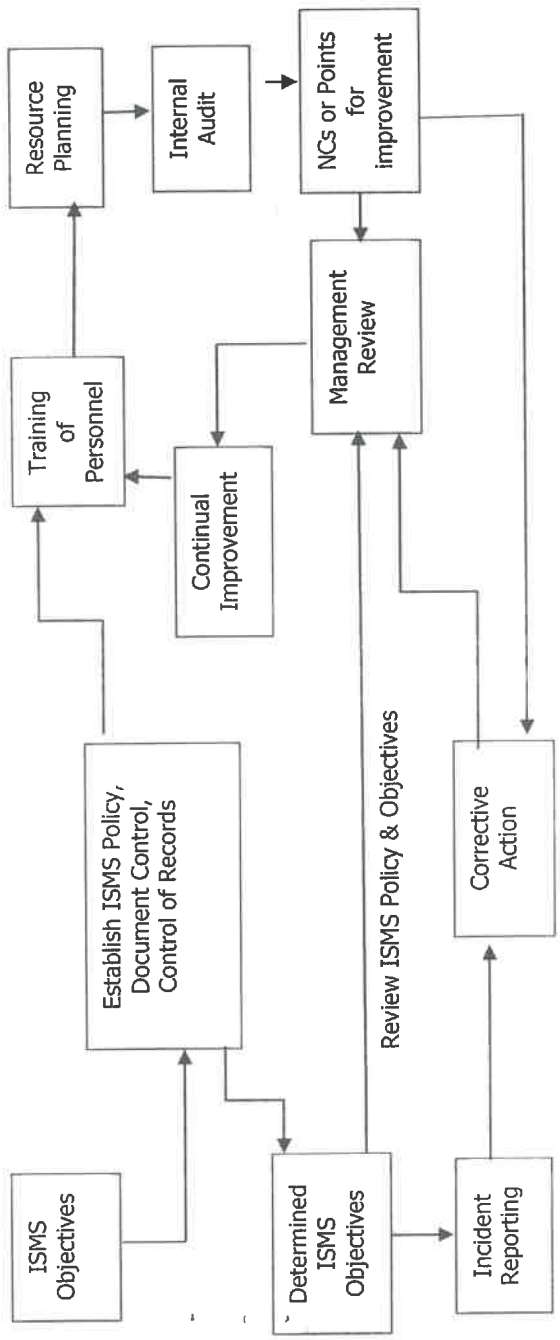
RISK & OPPORTUNITY IN ACHIEVING OBJECTIVES/ TARGETS

SR. NO.	RISK	OPPORTUNITY
1.	Shortage of Manpower	Recruitment / Stand by arrangement
2.	Non availability of suitable equipment/ resource needed.	Availability of suitable equipment/ resource needed.
3.	Noncompliance of statutory & regulatory directives and legal obligations.	Compliance of obligations applicable to the organization
4.	Non availability of suitable facilities	Availability of suitable facilities
5.	Issues raised by local authorities/leaders	Identify issues raised by local authorities/leaders in time
6.	Issues raised from nearby people	Identify Issues raised from nearby people in time



INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013

PROCESS FLOW CHART



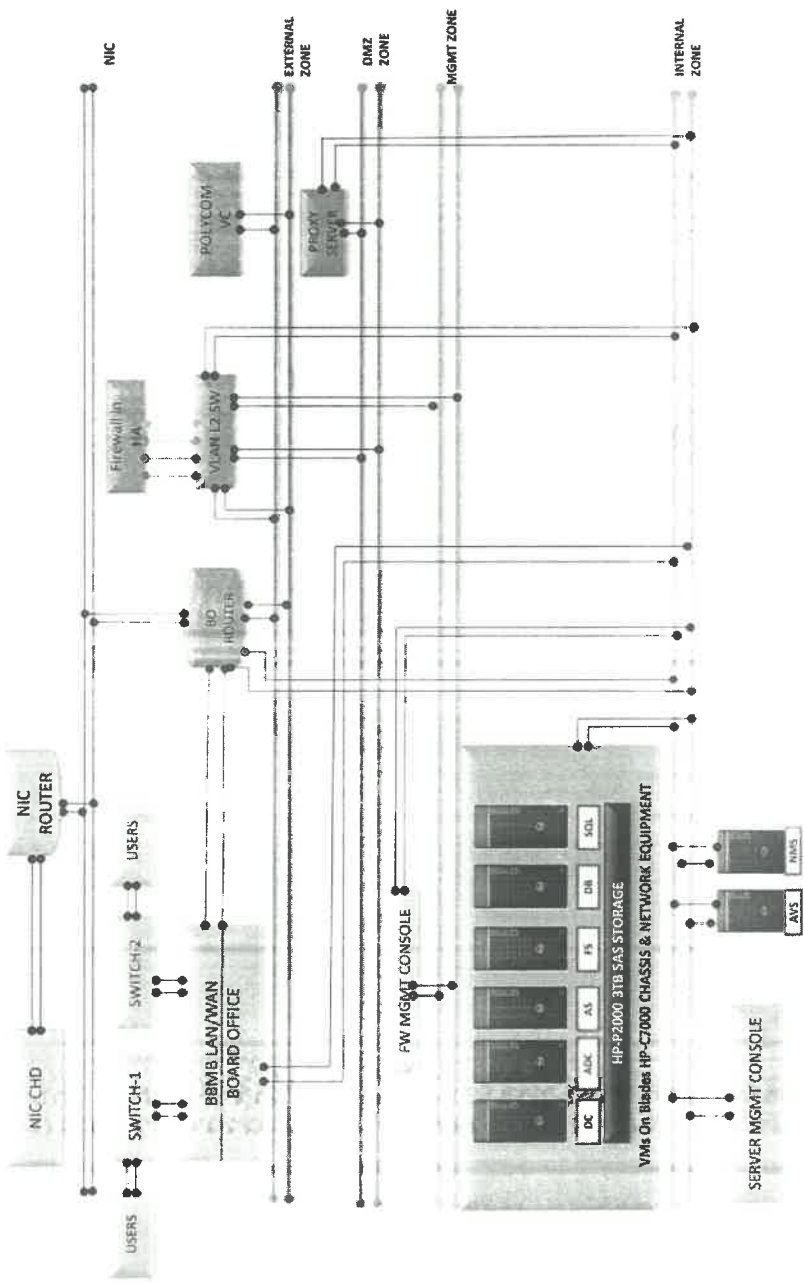
ISMS PROCESS FLOW FOR CONCERNED MR

Doc.No: ISMS/M/01 Sec no.: Annex-D	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 1 of 5
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILAIBLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				

**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

**NETWORK DIAGRAM**

1. BHAKRA BEAS MANAGEMENT BOARD (Computer Cell, National Hydrology Project (NHP), System Load dispatch Centre(SLDC)).



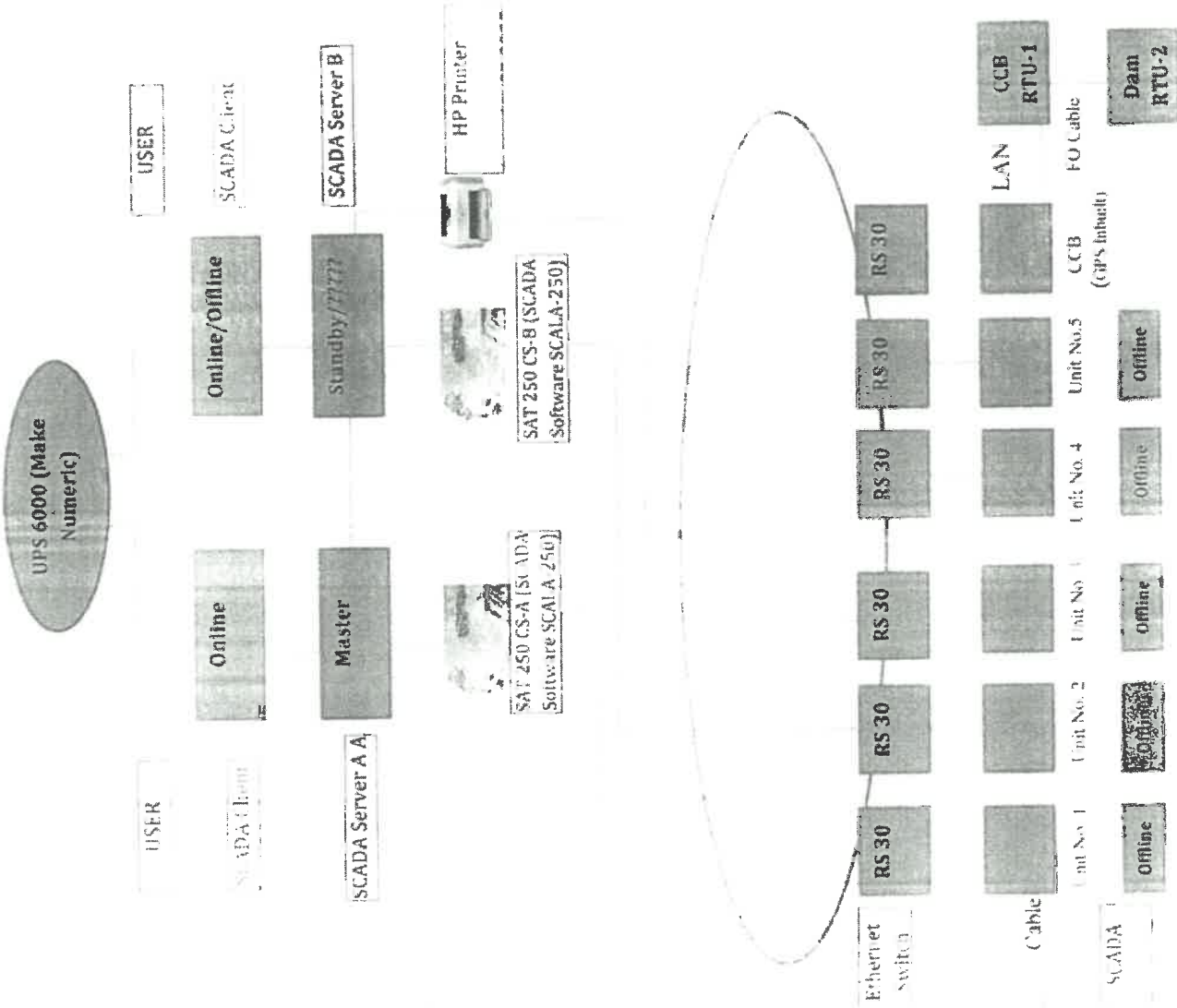
Doc.No: ISMS/M/01 Sec no.: Annex-D	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 2 of 5
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRS AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				



INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013

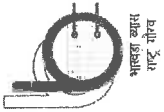
2. BHAKRA LEFT POWER HOUSE (SCADA SYSTEM OVERVIEW)

The network system diagram (Topology) is shown below:



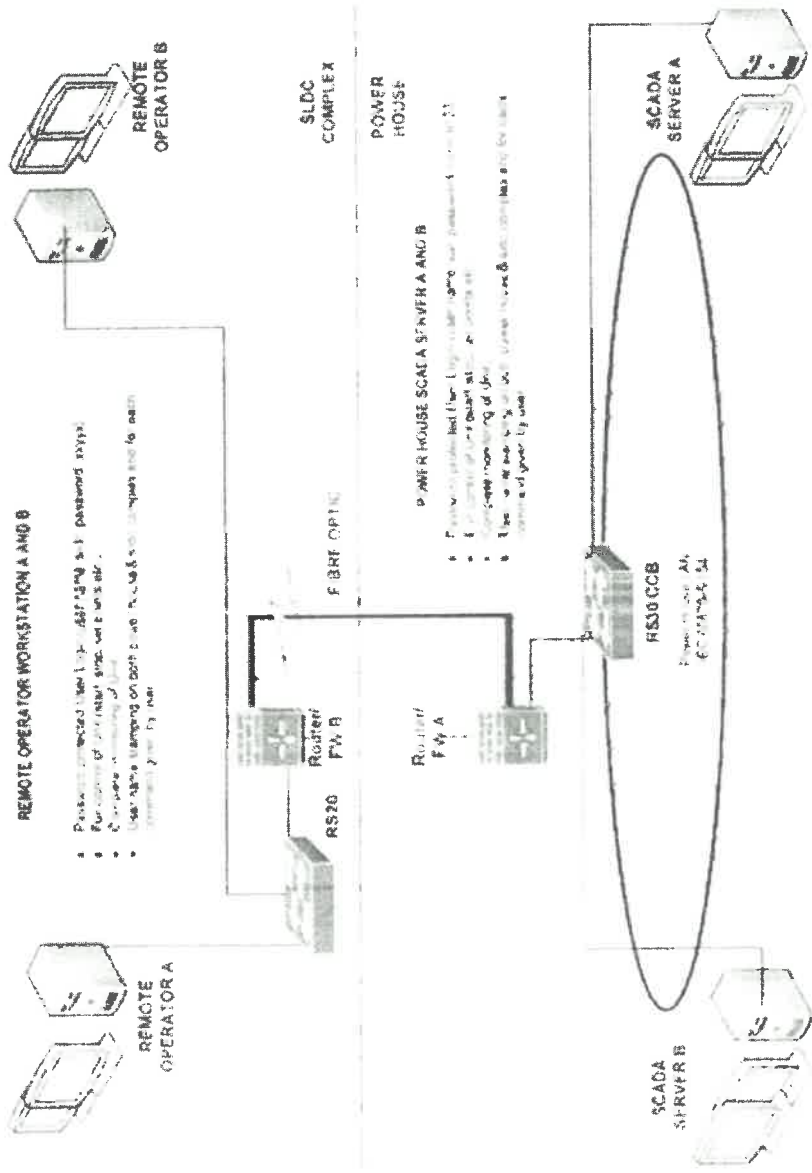
Doc.No: ISMS/M/01 Sec no.: Annex-D	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 3 of 5
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				





INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013

INTEGRATION OF BHAKRA LEFT BANK POWER HOUSE WITH REMOTE CONTROL ROOM OF BHAKRA LEFT POWER HOUSE AT SLDC CHANDIGARH



Doc.No: ISMS/M/01  
Sec no.: Annex-D

Revision No: 00

Issue No: 01

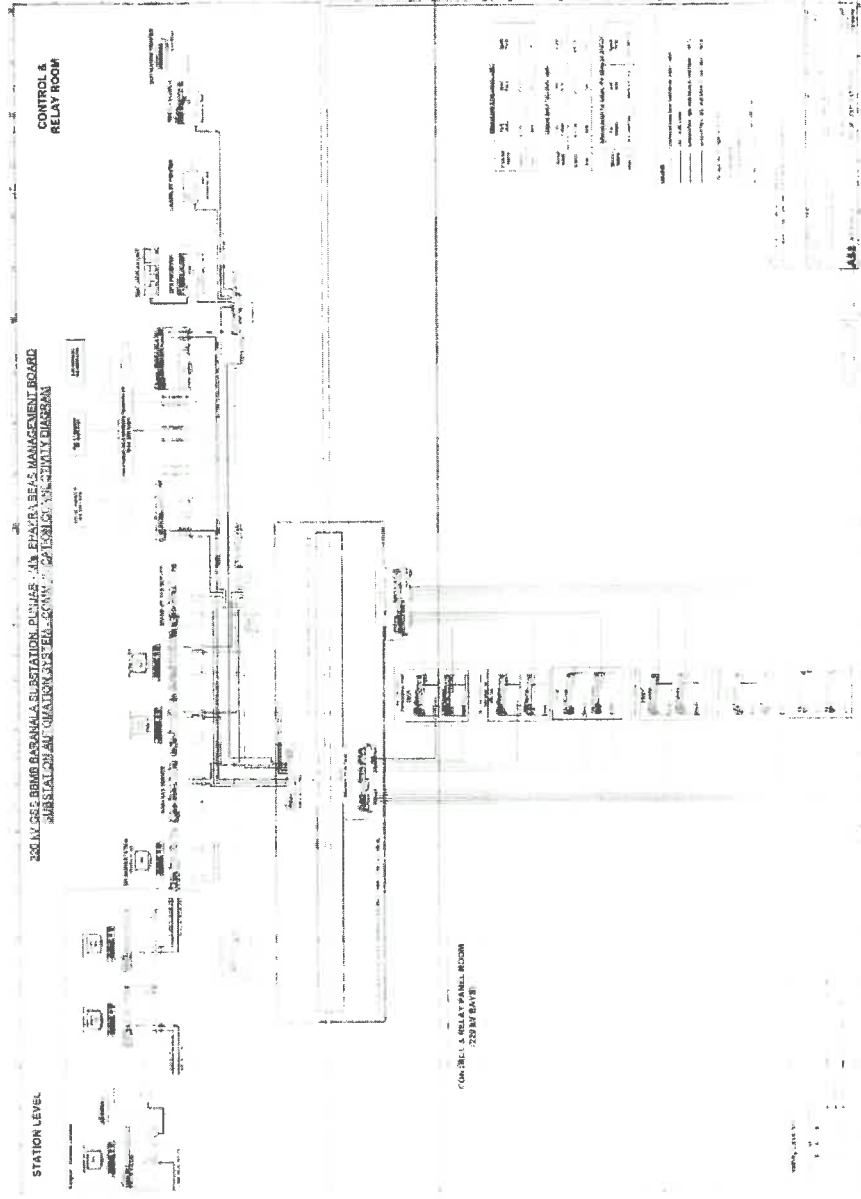
Rev. Date: NIL

Page 4 of 5

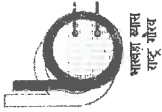
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET



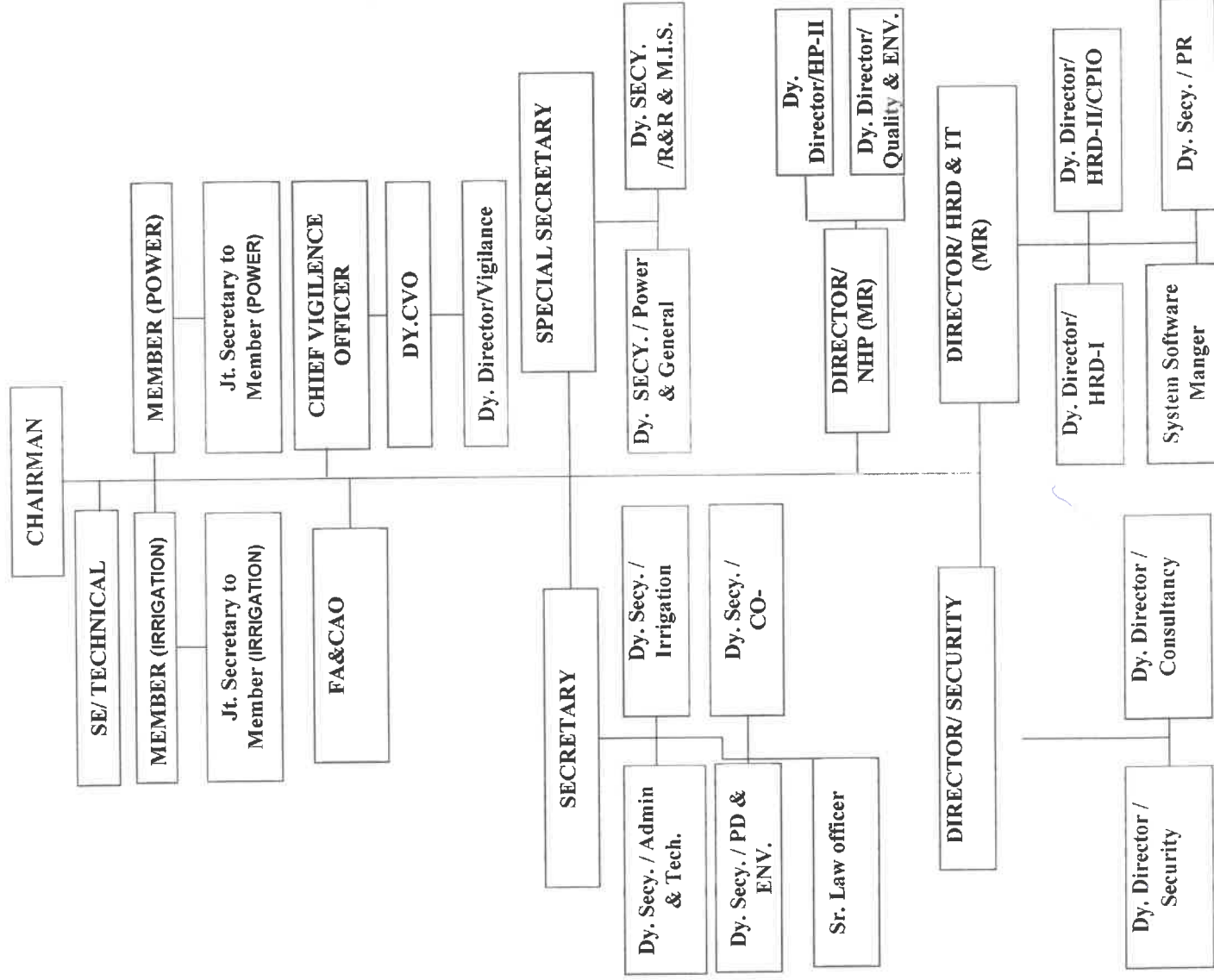
3. 220 KV SUBSTATION BARNALA (SAS) REMOTE OPERATIONS FROM 220 KV  
SUBSTATIONS SANGRUR.



Doc.No: ISMS/M/01 Sec no.: Annex-D	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 5 of 5
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN FROM OUT LATEST UPDATED COPY IS AVAILABLE WITH MRS AND AVAILABLE ON PASSWORD ENABLED WEBSITE AND BBMB INTRANET				



**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

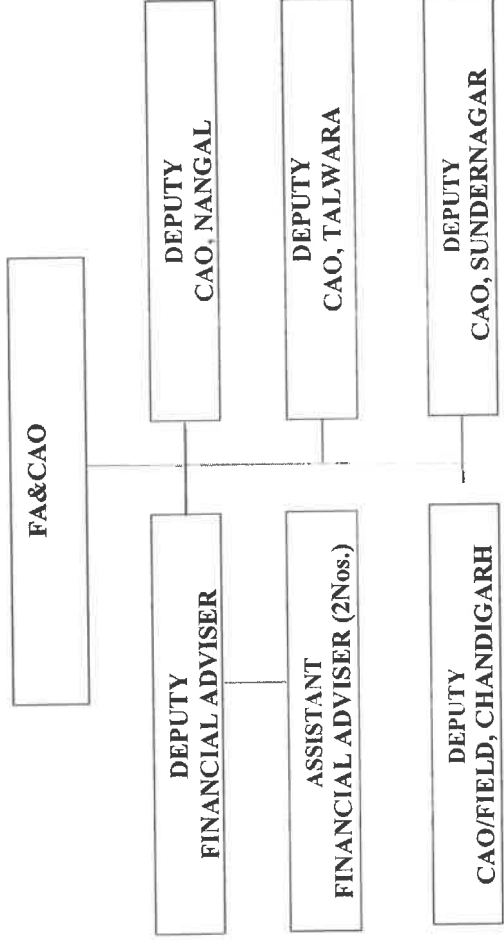


Doc.No: ISMS/M/01 Sec no.: Annex-E	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 1 of 4
---------------------------------------	-----------------	--------------	----------------	-------------

ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET



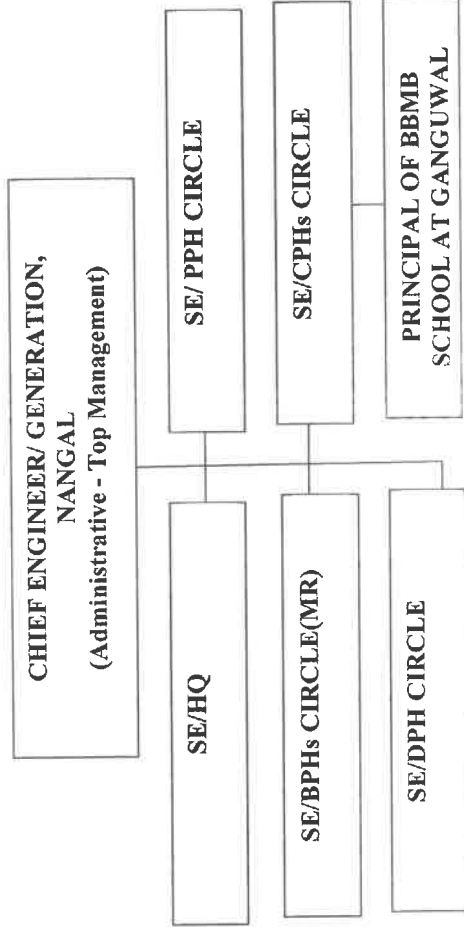
Organization set up of FA & CAO



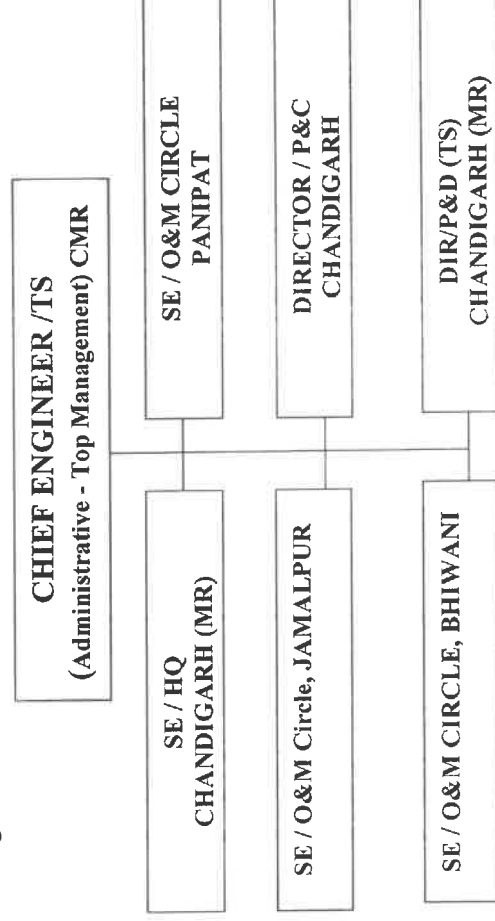
Doc.No: ISMS/M/01 Sec no.: Annex-E	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 2 of 4
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				



**A. Organization set up of Chief Engineer/Generation, Nangal (Power Wing)**



**B. Organizational set up of Chief Engineer/ Transmission System, Chandigarh (Power Wing)**

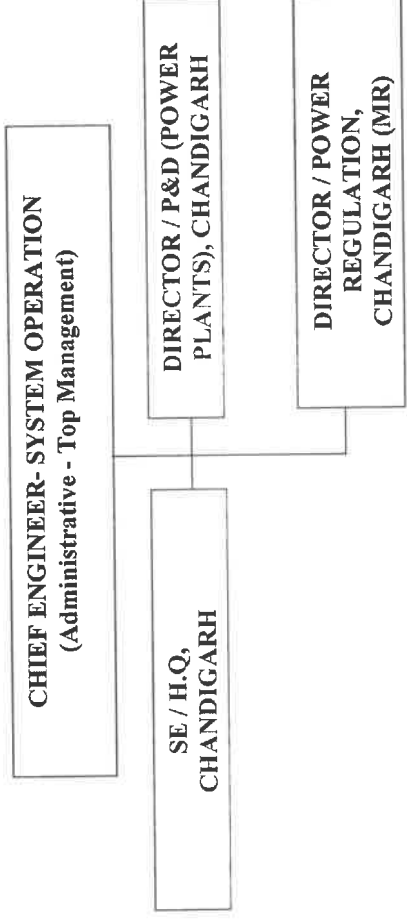


Doc.No: ISMS/M/01 Sec no.: Annex-E	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 3 of 4
---------------------------------------	-----------------	--------------	----------------	-------------

ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET



**C. Organization set up of Chief Engineer/System Operations, Chandigarh (Power Wing)**



Doc.No: ISMS/M/01 Sec no.: Annex-E	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 4 OF 4
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				



## ROLE, RESPONSIBILITY & AUTHORITY

### CE/TS, CMR:

#### Roles

Leading BBMB/TS  
Reporting to Regional MEMBER POWER.

#### Responsibility

Co-ordination/ liaison with State Govt. Authorities/ Local Administration, Public Leaders, Media, for resolution of various state level/local issues affecting the Power Transmission.

Monitoring of compliance of MOU and holding review meetings with departments & contractors.

To decide/ resolve technical, contractual issues including accord of approval of departmental proposals within his delegated powers and further processing such cases which are beyond his jurisdictions in accordance with provisions, extant rules and guidelines.

To ensure preparation/ finalization of annual plans, budgets etc.

To ensure implementation of social and other developmental activities at the Powerhouse /substations and its peripheries/ nearby localities.

To ensure timely submission of compliance obligations, various returns, reports, replies etc. to Regional/Corporate Office and other agencies.

To monitor Information Security Management System requirements by interacting with ISMS third party auditors/certification body etc.

To Chair the ISMS Team and approve the ISMS Policy.

#### Authority

Provide Guidelines and Directions.

#### Accountability

Failure in achieving objectives Failure in Information Security System within the boundary of BBMB, SAS, Computer Cell, SLDC, Substations.

Doc.No: ISMS/M/01, Sec no.: Annex-F	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 1 of 6
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				



### THE INFORMATION SECURITY STEERING COMMITTEE (ISSC)

- Information Security Steering Committee (ISSC) shall approve Bhakra Beas Management Board (BBMB) Information Security Policies based on recommendations from Security Forum (ISF).
- It shall plan, determine and provide the necessary resources (man power, tools, hardware, software, computing resources and information) for effective implementation of ISMS.

### ROLES AND RESPONSIBILITIES OF THE INFORMATION SECURITY FORUM (ISF)

- Review Security Incidents, significant change in facility/ operations, new business requirements, Legal and Regulatory requirements, Audit reports.
- Take appropriate actions based on the new security requirements.
- Identify the new threats and Risks based on above observations.

### ROLES AND RESPONSIBILITIES OF THE CHIEF INFORMATION SECURITY OFFICER (CISO)

- Manage the overall information systems security program in the organization.
- Develop the Information Systems Security Policies and Standards for use throughout the organization.
- Manage Risk Assessment and Risk Treatment process.
- Co-ordinate or Initiate the Security Forum Meetings for review and updating the Security Policies.
- Coordinate or Initiate Security Forum Meetings for effective Risk Assessment and Risk treatment process
- Ensure updation of the Information Asset Registers of the organization.

Doc.No: ISMS/M/01, Sec no.: Annex-F	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 2 of 6
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILAIBLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				

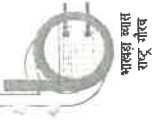


**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

सुरक्षा का  
रक्षक

- Keep Security Policies and Standards up to date, reflecting changes in technology, business direction and potential threats.
- Where necessary provide inputs to various departments in the development of specific standards or guidelines that meet the information security policies for specific products within the organization.
- Ensure that, when exceptions to the information security policy are necessitated, the risk acceptance process is completed and the exceptions are reviewed and re-assessed periodically.
- Remain current/up-to-date on the threats against the information assets (Attending information security meetings, reading trade publications and participation in work groups are some of the ways to stay current/up-to-date with the developments in the field of information systems security).
- Understand the current information processing technologies and the most current information protection methods and controls by receiving internal education, attending information security seminars and through on-the-job training;
- Understand the business processes of the organization, so as to provide appropriate security protection;
- Encourage the participation of the managers, auditors, legal experts and the staff members from other disciplines, who can contribute to the information systems security program
- Review audit and examination reports dealing with the information security issues and ensure that they are placed before the Steering Committee Meetings.
- Formulate the audit findings and follow-up to ensure that the security controls and procedures as required are implemented within the stipulated time frame.
- Assist in the preparation and distribution of an appropriate warning system of potentially serious and imminent threats/ attacks to the organization's information assets e.g. outbreak of computer virus etc.
- Co-ordinate or assist in the investigation of security threats or other attacks on the information assets;

Doc.No: ISMS/M/01, Sec no.: Annex-F	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 3 of 6
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILAIBLE WITH MRS AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				



- Assist in the recovery of information and information assets from attacks.

### **ROLES AND RESPONSIBILITIES OF THE DEPARTMENTAL INFORMATION SECURITY OFFICERS (DISOs)**

- Departmental Information Security Officer (DISO) could be a senior official who shall provide inputs for the design, development, implementation and maintenance of the Information Systems Security Program for protecting the information assets of the department.
- The DISO will have to:
  - Manage the overall information systems security program in concerned department or project.
  - Implement the Information Security policies through appropriate procedures for his department.
  - Monitor the security of resources and assets present in his department and safeguard against security breaches.
  - Monitor the judicious usage of resources.
  - Manage Security Incidents and escalate the security breaches to the CISO.
  - Remain current/up-to-date on the threats against the information assets (Attending information security meetings, reading trade publications and participation in work groups are some of the ways to stay current/up-to-date with the developments in the field of information systems security).
  - Understand the current information processing technologies and the most current information protection methods and controls by receiving internal education, attending information security seminars and through on-the-job training.
  - Encourage the participation of department members, for effective implementation of the information systems security program.
  - Review audit and examination reports dealing with the information security issues and ensures that corrective and preventive actions are formulated.

Doc.No: ISMS/M/01, Sec no.: Annex-F	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 4 of 6
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRS AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				

**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

सिस्टम सुरक्षा  
मंडळ, भोव

- Co-ordinate or assist in the investigation of security threats or other attacks on the information assets.
- Assist in the recovery of information and information assets from attacks.

**CONCERNED MR:**

Reporting to CMR if any major incident happened.  
Leading the team reporting to him  
Responsible for all activities related to his area of control  
Authorized in accordance with provisions, extant rules and guidelines.  
Accountable for failure in achieving objectives, failure in safety and security of all within his control.

**SE(HQ)/DIRECTORS:**

Reporting as per organizational hierarchy  
Leading the team reporting to him  
Responsible for all activities related to his area of control  
Authorized in accordance with provisions, extant rules and guidelines.  
Accountable for failure in achieving objectives, failure in safety and security of all within his control.

**(HR)**

Reporting as per organizational hierarchy  
Leading the team reporting to him  
Responsible for all activities related to his area of control  
Authorized in accordance with provisions, extant rules and guidelines.  
Accountable for failure in achieving objectives, failure in safety and security of all within his control.  
Participation in internal audit/MRM related to ISMS implementation.

**(Finance)**

Reporting as per organizational hierarchy  
Leading the team reporting to him  
Responsible for all activities related to his area of control  
Authorized in accordance with provisions, extant rules and guidelines.  
Accountable for failure in achieving objectives, failure in safety and security of all within his control.  
Participation in internal audit/MRM related to ISMS implementation.

Doc.No: ISMS/M/01, Sec no.: Annex-F	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 5 of 6
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILAIBLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				



**DDs/ADs/Engr's/AEs (All Sections of BBMB)**

Reporting as per organizational hierarchy  
Leading the team reporting to him  
Responsible for all activities related to his area of control  
Authorized in accordance with provisions, extant rules and guidelines.  
Accountable for failure in achieving objectives, failure in safety and security of all within his control.  
Participation in internal audit related to ISMS implementation

**Officers/Supervisors (All sections under BBMB)**

Reporting as per organizational hierarchy  
Leading the team reporting to him  
Responsible for all activities related to his area of control  
Authorized in accordance with provisions, extant rules and guidelines.  
Accountable for failure in achieving objectives, failure in safety and security of all within his control.  
Participation in internal audit related to ISMS implementation.

Doc.No: ISMS/M/01, Sec no.: Annex-F	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 6 of 6
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILABLE WITH MRS AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				



**INFORMATION SECURITY MANAGEMENT SYSTEMS MANUAL  
IS/ISO/IEC 27001:2013**

Index

**BBMB's Common ISMS Policies & Procedures.**

**Common Policies Document No.**

- |   |                                  |
|---|----------------------------------|
| 1. <u>Acceptable Usage Policy &amp; Procedure</u>             | Doc No: <u>BBMB/COM/ISM/P/01</u> |
| 2. <u>Access Control Policy &amp; Procedure</u>               | Doc No: <u>BBMB/COM/ISM/P/02</u> |
| 3. <u>Asset Enumeration &amp; Classification Policy</u>       | Doc No: <u>BBMB/COM/ISM/P/03</u> |
| 4. <u>Change Management Procedure</u>                         | Doc No: <u>BBMB/COM/ISM/P/04</u> |
| 5. <u>Clear Desk &amp; Clear Screen Policy</u>                | Doc No: <u>BBMB/COM/ISM/P/05</u> |
| 6. <u>Desktop Policy &amp; Procedure</u>                      | Doc No: <u>BBMB/COM/ISM/P/06</u> |
| 7. <u>Elect. Productivity &amp; Automatic Tools Policy</u>    | Doc No: <u>BBMB/COM/ISM/P/07</u> |
| 8. <u>Email Policy &amp; Procedure</u>                        | Doc No: <u>BBMB/COM/ISM/P/08</u> |
| 9. <u>Incident Response Policy &amp; Procedure</u>            | Doc No: <u>BBMB/COM/ISM/P/09</u> |
| 10. <u>Internet Access &amp; Usage Policy &amp; Procedure</u> | Doc No: <u>BBMB/COM/ISM/P/10</u> |
| 11. <u>Password Policy &amp; Procedure</u>                    | Doc No: <u>BBMB/COM/ISM/P/11</u> |
| 12. <u>Physical &amp; Environment Policy &amp; Procedure</u>  | Doc No: <u>BBMB/COM/ISM/P/12</u> |
| 13. <u>User Management Policy &amp; Procedure</u>             | Doc No: <u>BBMB/COM/ISM/P/13</u> |
| 14. <u>ISMS Glossary</u>                                      | Doc No: <u>BBMB/COM/ISM/W/01</u> |

Doc.No: ISMS/M/01, Sec no.: Annex-G	Revision No: 00	Issue No: 01	Rev. Date: NIL	Page 1 of 1
ISMS MANUAL IS TREATED AS UNCONTROLLED IF TAKEN PRINTOUT. LATEST UPDATED COPY IS AVAILAIBLE WITH MRs AND AVAILABLE ON PASSWORD ENABLED WEBLINK AND BBMB INTRANET				