PUNJAB STATE WAREHOUSING CORPORATION

PSWC IT POLICY

[Version 1.1]

INDEX

1. About the Information Technology Policy

PSWC provides and maintains technological products, services and facilities like Personal Computers (PCs), peripheral equipment, servers, Internet and application software to its users for official use. The Information Technology (IT) Policy of the organization defines rules, regulations and guidelines for proper usage and maintenance of these technological assets to ensure their ethical and acceptable use and assure health, safety and security of data, products, facilities as well as the people using them. It also provides guidelines for issues like purchase, compliance, IT support and grievance redressal of the users pertaining to technological assets and services used for office work.

1.1 Definition

In this Policy, the following words and expressions, unless inconsistent with the context, shall bear the meanings assigned thereto:

1.1.1 "**IT Policy**" : IT Policy is a set of rules and guidelines on how IT resources should be used, and how daily operations should be conducted.

1.1.2 "**Information Technology**" : Information technology (IT) is the use of any computers, storage, networking and other physical devices, infrastructure and processes to create, process, store, secure and exchange all forms of electronic data. Typically, IT is used in the context of business operations, as opposed to technology used for personal or entertainment purposes. The commercial use of IT encompasses both computer technology and telecommunications.

1.1.3 "**IT Equipment**" : Information Technology Equipment is a group or "family" of products, which include devices that have a primary function related to the collection, transfer, storage, or processing of data.

1.1.4 "**Management Committee**" : The Management Committee is the group of officials who are held accountable for the activities of the organization. It is the ultimate decision-making forum.

1.1.5 "**IT Wing**" : The IT Wing i.e. Computer Branch of PSWC, Head Office, which involves in compliance of all IT related policies in PSWC. It is responsible to study, develop and rolling out new software modules and mobile apps in PSWC. It purchases new IT hardware & Software for PSWC as per requirements and manages its inventory. It also manages PSWC portal. It provides training and IT support to all its end users. It also oversees the installation & maintenance of IT hardware and ensure its smooth functioning. It also arranges & manages regular meeting using Video conferencing.

1.1.6 "**Equipment Eligibility**" : Define guidelines / rules for proper allocation of IT Equipment or IT resources among various level of users for optimum utilization of IT resources .

1.1.7 "**Residual Value**" : Residual Value is the estimated value of a IT Equipment at the end of its lease term or useful life.

1.1.8 "**Life Span**" : Life span refers to IT equipment has a period within which it operates at its best before it becomes obsolete.

1.1.9 "**Condemnation**" : IT hardware completed its life span from the date of purchase, if declared fit for disposal or may be retained by the allotted user.

1.1.10 "**Disposal**" : IT hardware completed its life span from the date of purchase and allotted user not willing to retain it, then, if declared fit for disposal as per e-waste policy.

1.1.11 "**Competent Authority**" : is any official that has the legally delegated or power to perform a designated function.

1.1.12 "**Internet Usage**" : Internet usage is the measurement (expressed in bytes, kilobytes, megabytes or gigabytes) of the amount of data flowing through the computer and the Internet network for a defined period.

1.1.13 "**Access Control**" : Access Control is a fundamental component of data security that dictates who's allowed to access and use PSWC information and resources.

1.1.14 "**Intrusion Detection**" : An intrusion detection is a device or software application that monitors a network for malicious activity or policy violations.

1.1.15 **"Critical Information Infrastructure**" : is defined as "the computing & other resources, the incapacitation or destruction of which, shall have debilitating impact on security or safety of e-Governance application & databases of PSWC."

1.1.16 "**Asset Register**" : is a complete listing of a business' or an entity's physical IT Equipment / resources.

1.1.17 "**Risk Analysis**" : Risk analysis involves examining how project outcomes and objectives might change due to the impact of the risk event.

1.1.18 "**Business Continuity Plan" :** A business continuity plan is a process that outlines the potential impact of disaster situations, creates policies to respond to them and helps businesses recover quickly so they can function as usual

1.1.19 "**Disaster Recovery**" : Disaster recovery is an organization's method of regaining access and functionality to its IT infrastructure after events like a natural disaster, cyber attack, or even business disruptions.

1.1.20 "**Backup Plan**" : A backup plan is a strategy of creating a copy of data that can be recovered and restored in case the original is lost or corrupted.

1.1.21 "**Systems** " : A system is an organized collection of parts (or subsystems) that are highly integrated to accomplish an overall goal. The system has various inputs, which go through certain processes to produce certain outputs, which together, accomplish the overall desired goal for the system.

1.1.22 "**GUI** " : Graphical user interface (GUI), a computer program that enables a person to communicate with a computer through the use of symbols, visual metaphors, and pointing devices.

1.1.23 "**Change Request**" : A change request is a formal proposal for an alteration to some product or system. In project management, a change request often arises when the client wants an addition or alteration to the agreed-upon deliverables for a project.

1.2 Purchase

Purchasing all IT Hardware and Software shall be done as per the Financial Rules and Procedure followed by PSWC from time to time.

1.3 Employee Training

1.3.1 Basic IT proficiency training as per latest trending technology is provided to all employees of Group A, B & C (minimum 12 hours per year)

1.3.2 Employees can also request and/or the IT Wing can decide to conduct additional training bases on a regular or requirement basis.
1.3.3 Training can be outsourced / In-house.

1.4 Incident Reporting & Resolution

1.4.1 PSWC uses multiple Graphical user interface GUIs (Mobile App, Web based applications) for incident reporting, all connected to a common database.
1.4.2 All end users will request all IT related issues via these GUIs only.
1.4.3 These GUIs shall be monitored by IT Wing.
1.4.4 In case of down time of these GUIs, all incidents shall be reported through e-office.
1.4.5 A ticket shall be assigned on reporting of an incident and shall carry the following details :

- Ticket No.
- Resolution time
- Issue reported date & time
- Issue reported by
- Issue details

1.4.6 The following shall be the resolution timelines as per the category of incident reported :

S.No.	Category of Issue	Type	Resolution Timeline
1	Software	In-house Software Application	24 hours
2	Software	Third party software application	48 hours
4	Hardware	Replacement with in stock item	24 hours
5	Hardware	Replacement with new item <= Rs. 10,000/- (not in stock)	48 hours
6	Hardware	Replacement with new item > Rs. 10,000/- and <= Rs. 1,00,000/- (not in stock)	15 working days
7	Hardware	Replacement with new item > Rs. 1,00,000/- and <= Rs. 5,00,000/-	30 working days
8	Hardware	Replacement with new item > Rs. 5,00,000/- (not in stock)	60 working days

Issues related to software application shall not include new change requests which involve changes in logic / re-writing of code / procurement of new resource to support the business continuity, change requests shall be dealt as per clause (8).

2. Equipment Usage Policy

2.1 Objective

The Equipment Usage policy informs employees and managers about equipment purchase, organizational and project-level inventory management, rules for allocating & transferring equipment to employees, departments or projects and best practices for all equipment usage and maintenance.

2.2 Equipment Listing

The following equipment is listed for purchase / development for issuance by the organization for the employees, departments or projects for their official use. The list is fully but not limited to

a. Personal Computing Devices (Desktop, Laptop, Tablet)
b. Computer Peripherals (Printer, Scanner, Photocopier, Fax Machine, Keyboard, Mouse, Web Camera, Speaker, Modem etc.)
c. Networking Equipment & Supplies (Router, Switch, Antenna, Wiring, etc.)
d. MS Office, PDF Reader
e. Any third party software as on need basis
f. Accessing the PSWC Portal as per user roles.

3. Equipment Eligibility

PSWC Policy guidelines for provision of Desktop Computers/Laptops// Tablets/printers/scanners/Software to the officials of PSWC posted at Head Office & Field offices.

S. No.	Item	Eligibility	Qty Entitled upto	Sanctioned Limit Upto (In Rs.)	Procurement Level	Minimum Configuration	Minimum Warranty (Year)
1	Desktop PC	All Group B & C employees except Godown Attendant, and Driver	1	75,000/-	IT Wing, Head Office	Annexure - A	Three
		Group A employees, Branch Manager/ IT Wing Head	1	1,50,000/-	IT Wing, Head Office	Annexure – A1	Three
2	Laptop	a) Branch Manager / IT Wing Head	1	1,00,000/-	In case of District Manager, Addl. District Manager, Technical Officer, AAO, Branch Manager/ IT Wing Head, to be purchased by officials themselves as per policy. The amount shall be reimbursed on submission of original	Annexure – B	Three
		b) IT Team Member	1				
		c) District Manager	1	70,000/-			
		d) AAO	1				
		e) Technical Officer	1				
		f) Addl. District Manager	1				

					bills.		
		g) Centre Incharge of Warehouse (Field)	1	70,000/-	In case of Centre Incharge and IT Team, to be purchased by IT Wing Head Office. The laptop shall be property of the respective Warehouse office only.		
3	Printers	a) Head Office Branch	2	30,000/-	IT Wing, Head Office	Annexure - C	One
		b) District Office	3				
		c) Centre Incharge	2				
4	Scanners	a) Head Office Branch	1	20,000/- To 50,000/-	IT Wing, Head Office	Annexure – D	One
		b) District Office	1				
		c) Centre Incharge	1				
5	Photocopy Machines	a) Head Office Branch	1 for 2 Branches	-	On Outsourcing Basis. Annual Contract to be done by District Manager for District Office & by IT Wing for Head Office following due financial procedure.		
		b) District Office	1				
6	Internet Facility	a) Head Office Branch	35 Mbps	As per prevailing rates of ISP	IT Wing, Head Office		One
		b) District Office	10 Mbps		District Office		One
		c) Centre Incharge	8 Mbps		District Office		One
7	Internet Data Card	a) IT Team Member b) Branch Manager/ IT Wing Head c) AAO d) District Manager e) Technical Officer f) Addl. District Manager g) O/o of Managing Director & Addl. Managing Director h) O/o of The Chairman	1	1,000 Per Internet Data Card (Inclusive of all taxes and charges)	IT Wing, Head Office		NA
8	UPS	a) Head Office	1	As per need basis post approval from the Competent Authority	IT Wing, Head Office	Online of 20 KVA	One
		b) District Office	1		IT Wing, Head Office	Online of 2 KVA	
		c) Centre Warehouse	2		IT Wing, Head Office	Offline of 1 KVA	
9	Third Party Software	All Employees	As per need basis		IT Wing, Head Office		
10	PSWC Portal	All Employees	As per user role	As per user role	IT Wing, Head Office		
11	VC Equipment	a) Head Office	1	As per need basis	IT Wing, Head Office		One
		b) District Office	1	As per need basis	IT Wing, Head Office		One

12	CCTVs & Supporting equipment	Warehouse campus	5	As per need basis post approval from the Competent Authority	IT Wing, Head Office	As per latest market trend	1
		Head office	As per need basis				
13	Video wall & Supporting equipment	As per need basis	As per need basis	As per need basis post approval from the Competent Authority	IT Wing, Head Office	As per latest market trend	1

3.1 Re-imbursement

Reimbursement to the officials mentioned in eligibility clause 3 2.(a),(c),(d),(e) & (f) shall be made by Punjab State Warehousing Corporation through RTGS in his/her bank account (as mentioned in Laptop Request Form) only after purchase of Laptop or any other computer peripherals hardware, on submission of bills & due approval of competent authority.

3.2 Calculation of Residual Value

The following table shows year wise matrix for calculating Residual Value from purchase value of IT Hardware.

(Matrix)

IT Hardware	**Completion Year Wise Rate of Calculating Residual Value**						
	Year-1	Year-2	Year-3	Year-4	Year-5	Year-6	**Beyond 6 Years**
All IT Hardware (Except Printer, Scanner & Laptops procured under Laptop policy 2017)	**90%**	**70%**	**60%**	**40%**	**20%**	**10%**	**5%**
Printer	**90%**	**70%**	**40%**	**20%**	**10%**	**5%**	**5%**
Scanner	**90%**	**70%**	**40%**	**20%**	**10%**	**5%**	**5%**

(The residual value of the Laptops/tablets procured by officers under previous Laptop Policy-2017 shall be calculated as per terms & conditions of the same Policy i.e. Laptop Policy 2017 only)

3.3 Equipment Life Span

The life span of IT (hardware & software) has been fixed for six years except printer (life span is 3 years), scanner (life span is 2 years). Accordingly, based on lifespan, year wise residual value matrix has been derived for calculating prevailing residual

value of any IT hardware item. There is no life span for third party software and in-house developed software. The same shall be upgraded as per guidelines of latest advanced technology.

3.4 Replacement

3.4.1 In case any IT hardware, issued to allotted user, completes its life span, the IT Wing, PSWC will ensure to replace such IT hardware item(s) as per the policy. In case the IT hardware has been procured by the user on re-imbursement basis such as laptop by Branch Managers / IT Wing Head / District Managers / AAOs, user shall submit written request for replacement.

3.4.2 The allotted user can seek the replacement of Laptop on completion of six years period from the date of purchase of Laptop.

3.4.3 Whenever an allotted user seeks to replace an IT hardware on completion of its lifespan of six years, he/she will have the option to either return the used/ old IT hardware to the Department or retain the same for his/her personal use after depositing its residual amount. Laptop can be retained by the concerned official only after completion of its lifespan.

3.4.4 In case of laptop, if the employee is retiring within residual value period i.e. before six years of purchase of laptop, he/she will have the option to deposit the residual amount and retain allotted laptop subject to approval of the Competent Authority.

3.5 Surplus & Transfer

In case IT Hardware issued to any official of PSWC, becomes surplus, IT Wing Head, PSWC shall be authorized to take appropriate decision for surplus IT hardware and shifting of such IT Hardware as per requirement to any other location.

3.6 Condemnation

3.6.1 Wherever the IT hardware item has completed its life span from the date of purchase, it shall be declared fit for condemnation only after analysis by committee of CTO, Manager (Storage) or representative, MFA or representative.

3.6.2 The IT hardware item(s), once declared fit for condemnation or declared unfit for continued use in the offices, may be offered to the allotted officials as per first priority at the depreciated value as applicable in each category. In case the official is not interested in procuring the same, the hardware item shall be auctioned within PSWC through an online (in-house) auction platform and shall be given away at the best offer price. In case the auction does not mature, IT hardware items shall be disposed off as per the latest e-waste policy of Govt. of Punjab.

3.7 Disposal of Condemned Equipment (IT Hardware Item(s))

3.7.1 In case of IT hardware, is declared condemned except printer, scanner & UPS, after completing its life span from the date of purchase, the allotted user will have the option to retain the same, on depositing residual amount as per Clause (4), for personal use. In case the official is not interested in procuring the same, the hardware item shall be auctioned within PSWC through an online (in-house) auction platform and shall be given away at the best offer price. In case the auction does not mature, IT hardware items shall be disposed off as per the latest e-waste policy of Govt. of Punjab.

3.7.2 In case of printer, scanner or UPS is declared condemned after completing its life span, the hardware item shall be auctioned within PSWC through an online (in-house) auction platform and shall be given away at the best offer price. In case the

auction does not mature, IT hardware items shall be disposed off as per the latest e-waste policy of Govt. of Punjab.

3.7.3 A central store will be set-up at PSWC Head Office, Chandigarh for the storage of condemned IT hardware.

3.7.4 The IT Wing in any case, would maintain the inventory of all purchases and disposal of all these items. For this purpose, IT Inventory Management software has been implemented for managing all IT hardware & software equipments.

4. General Guidelines

4.1 **Equipment** (IT Hardware – For Laptops Purchased by Officers (Branch Manager / IT Wing Head / IT Team Member / District Manager / AAO / Technical Officer / Additional District Manager) on Re-imbursement Basis.

4.1.1 Procurement shall be done by the officer concerned directly from the Original Equipment Manufacturer (OEM) or their authorized dealers within 30 days from the date of sanction.

4.1.2 Laptop purchased must meet the minimum specification as mentioned in Annexure-B of this policy.

4.1.3 Laptop shall be bought with three years comprehensive warranty.

4.1.4 Officer shall ensure that due care has been taken to avail to best price and other available benefits.

4.1.5 The officer can procure the Laptop costing any amount higher or lesser than the sanctioned limit. However, concerned officer shall bear the additional cost over and above the sanctioned limit, if any. In case the officer buys lesser than the sanctioned amount, then actual cost of laptop shall be considered for reimbursement.

4.1.6 The overall cost limit shall include the cost of anti-virus software.

4.1.7 The officer shall be wholly responsible for ensuring that documents submitted at the time of submitting utilization certificate are genuine & authenticated, which may be verified by the concerned department.

4.1.8 Eligible officer shall send his request (as per Format-1) for Laptop to the Computer Branch.

4.1.9 Managing Director of the PSWC may also sanction the purchase of Laptop for any other officer of his/her department on need basis under this policy.

4.1.10 Officer shall give a declaration at the time of making request for Laptop that no other Laptop(s) has(ve) been issued to him/her by any office of any other State Department/ Board/ Commission/ Society/ Corporations/ any other State owned agency or Public Sector Undertaking.

4.1.11 There shall be no provision of any claim regarding write-off of laptop on account of theft.

4.1.12 Officers / Officials on contract / deputation shall be issued / sanctioned laptop only subject to the approval of the Managing Director.

4.2 Equipment (IT Hardware)

4.2.1 PSWC shall not be responsible/ liable for any contractual, legal and statutory, cyber security issues arising out during the use of IT hardware.

4.2.2 PSWC shall be responsible to make all necessary entries of IT hardware in their stock record.

4.2.3 Procurement of IT hardware / services, beyond the scope of this policy or left escaped, shall subject to approval of the Competent Authority.

4.2.4 This policy shall supersede any earlier letter/instructions/ policy/ guidelines etc. issued regarding allotment of IT hardware / services in PSWC.

5. Equipment (IT Hardware & Software) - Inventory Management

5.1 The IT Wing is responsible for maintaining an accurate inventory of all technological assets, software and tangible equipment purchased by the organization.

5.2 The following information is to be maintained for above mentioned assets in an Inventory Sheet:

a. Item
b. Brand/ Company Name
c. Serial Number
d. Basic Configuration (e.g. HP Laptop, 500 GB HD, 4 GB RAM etc.)
e. Physical Location
f. Date of Purchase
g. Approving Authority
h. Purchase Cost
i. Allotted to

5.3 When an Inventory Sheet is updated or modified, the previous version of the document should be retained. The date of modification should be mentioned in the sheet.

5.4 Inventory audits (minimum once in a year) will be carried out by the IT Wing to validate the inventory and make sure all assets are up-to-date and in proper working condition as required for maximum efficiency and productivity.

5.5 Equipment Allocation, De-allocation & Relocation

5.5.1 Allocation of Equipment (IT Hardware & Software)

a. Employees may be allocated equipment as per their eligibility criteria mentioned in 3.1.
b. If required, employees can request through the Reporting Manager(s) for additional equipment or supplies like external keyboard, mouse etc.
c. No employee is allowed to carry official equipment out of office (Except sanctioned laptop).

5.5.2 De-allocation of Assets

a. It is the Reporting Manager's responsibility to collect all allocated organizational equipment & other assets from an employee who is leaving the organization.
b. IT Wing shall ensure updating the Inventory Sheet mandatory after receiving back all allocated equipment.

6. Internet Usage Policy

6.1 Objective

The Internet Usage Policy provides guidelines for acceptable use of the organization's Internet network so as to devote Internet usage to enhance work productivity and efficiency and ensure safety and security of the Internet network, organizational data and the employees.

6.2 General Guidelines (Head Office)

6.2.1 Internet is a paid resource and therefore shall be used only for office work.
6.2.2 The organization reserves the right to monitor, examine, block or delete any/all incoming or outgoing internet connections on the organization's network.
6.2.3 The PSWC Head Office has systems in place to monitor and record all Internet usage on the Head Office network including each website visit. The Management Committee can choose to analyze Internet usage and publicize the data at any time to assure Internet usage is as per the IT Policy.
6.2.4 The organization has installed an Internet Firewall at Head Office to assure safety and security of the organizational network. Any employee who attempts to disable, defeat or circumvent the Firewall will be subject to strict disciplinary action.

6.3 Internet Login Guidelines (Head Office)

6.3.1 All employees may be provided with a Username and Password to login to the Internet network in the office.
6.3.2 An employee can also get a local static IP address for internet and intranet use. For IOS based devices UDID no. is added in order to use all PSWC Apps.
6.3.3 Username and password for a new employee must be requested by the Reporting Manager.
6.3.4 Sharing the Username and Password with another employee, visitor or guest user is prohibited.
6.3.5 A visitor or guest user who wants to use the office Internet will be given a Guest Username and Password.
6.3.6 Any password security breach must be notified to the IT Wing immediately.
6.3.7 Username and password allotted to an employee will be deleted upon resignation/termination/retirement from the organization.

6.4 Password Guidelines

The following password guidelines can be followed to ensure maximum password safety.

6.4.1 Select a Good Password:

a. Choose a password which does not contain easily identifiable words (e.g. your username, name, phone number, house location etc.).
b. Use 8 or more characters.
c. Use at least one numeric and one special character apart from letters.
d. Combine multiple unrelated words to make a password.

6.4.2 Keep your Password Safe:

a. Do not share your password with anyone.
b. Make sure no one is observing you while you enter your password.
c. As far as possible, do not write down your password. If you want to write it down, do no display it in a publicly visible area.
d. Change your password periodically (every 3 months is recommended).

e. Do not reuse old passwords. If that is difficult, do not repeat the last 5 passwords.

6.4.3 Other Security Measures:

a. Ensure your computer is reasonably secure in your absence.
b. Lock your monitor screen, log out or turn off your computer when not at desk.

6.4.4 Online Content Usage Guidelines

Employees are solely responsible for the content accessed and downloaded using Internet facility in the office. If they accidentally connect to a website containing material prohibited by the organization, they should disconnect from that site immediately.

6.4.5 Inappropriate Use

The following activities are prohibited on organization's Internet network. This list can be modified/updated anytime by the IT Wing as deemed fit. Any disciplinary action considered appropriate by the Management Committee (warning/legal action / termination etc.) can be taken against an employee involved in the activities mentioned below:

6.4.5.1 Playing online games, downloading and/or watching games, videos or entertainment software or engaging in any online activity which compromises the network speed and consumes unnecessary Internet bandwidth
6.4.5.2 Downloading images, videos and documents unless required to official work
6.4.5.3 Accessing, displaying, uploading, downloading, storing, recording or distributing any kind of pornographic or sexually explicit material unless explicitly required for office work
6.4.5.4 Accessing pirated software, tools or data using the official network or systems
6.4.5.5 Uploading or distributing software, documents or any other material owned by the organization online without the explicit permission of the Competent Authority.
6.4.5.6 Engaging in any criminal or illegal activity or violating law
6.4.5.7 Invading privacy of coworkers
6.4.5.8 Using the Internet for personal financial gain or for conducting personal business
6.4.5.9 Deliberately engaging in an online activity which hampers the safety & security of the data, equipment and people involved.
6.4.5.10 Carrying out any objectionable, frivolous or illegal activity on the Internet that shall damage the organization's reputation.
6.4.5.11 Use of any type of social media and use of YouTube.

7. Information Security Policy

7.1 Objective

Information security means protection of the organization's data, applications, networks and computer systems from unauthorized access, alteration and destruction. The Information Security Policy provides guidelines to protect data integrity based on data classification and secure the organization's information systems.

7.2 General Guidelines

7.2.1 Various methods like access control, authentication, monitoring and review will be used to ensure data security in the organization.

7.2.2 Security reviews of servers, firewalls, routers and monitoring systems must be conducted on a regular basis minimum once in a year. These reviews should include monitoring of access logs and intrusion detection software logs.

7.3 Data Classification

7.3.1 The organization classifies data into three categories:

a. High Risk:

i. It includes information assets which have legal requirements for disclosure and financial penalties imposed for disclosure.

ii. E.g. Payroll, personnel, financial, biometric data

b. Medium Risk:

i. It includes confidential data which would not impose losses on the organization if disclosed, but is also not publicly available.

ii. E.g. Agreement documents, unpublished reports, etc.

c. Low Risk:

i. It includes information that can be freely disseminated.

ii. E.g. brochures, published reports, other printed material etc.

7.3.2 Different protection strategies would be developed by the IT Wing for the above three data categories. Information about the same must be disseminated appropriately to all relevant departments and staff.

7.3.3 High risk data must be encrypted when transmitted over insecure channels.

7.3.4 All data must be backed up on a regular basis as per the rules defined by the IT Wing at that time.

7.4 Access Control

7.4.1 Access to the network, servers and systems in the organization will be achieved by individual logins and will require authentication. Authentication includes the use of passwords, biometrics or other recognized forms of authentication.

7.4.2 All users of systems which contain high or medium risk data must have a strong password as defined in the IT Policy.

7.4.3 Default passwords on all systems must be changed after installation.

7.4.4 Where possible and financially feasible, more than one person must have full rights to any organization-owned server storing or transmitting high risk and medium risk data.

7.5 Virus Prevention

7.5.1 All servers and personal computers that connect to the network must be protected with centralized licensed anti-virus software recommended by the vendor. The software must be kept up-to-date.

7.5.2 Whenever feasible, system/network administrators must inform users when a virus/ other vulnerability has been detected in the network or systems.

7.6 Intrusion Detection

7.6.1 Intrusion detection must be implemented on all servers and workstations containing high and medium risk data.

7.6.2 Operating system and application software logging process must be enabled on all systems.

7.6.3 Server, firewall and critical system logs should be reviewed frequently.

8. Change Request

8.1 A change or addition in the systems (Software applications / Hardware etc) supporting the business continuity, can be requested to enhance / improve the system.

8.2 Changes can be requested to the IT Wing by the Branch Heads / District In-charge / PSWC related departments or can also be ordered by the MD/AMD/BOD/ GOP/ GOI.

8.3 Whenever a change request is received by the IT Wing, it shall be analyzed for impact / reform benefits and study document along with implementation schedule shall be prepared accordingly.

8.4 The document shall be duly vetted by the end user branch or a committee formed by the Competent Authority before bringing the same in to implementation.

8.5 Approval shall be sought for the same for implementing the change request as below:

S.No.	Change Request	Approval Level
1	Relating to change/modification in the existing system	AMD
2	Relating to new introductions	MD

8.6 After any change request / new addition is incorporated, the end user shall be informed (if required) through a release document having details of the same

8.7 All change requests / new additions to the system shall be tested on pilot basis before release (minimum for 7 days) and the testing report, shall be apprised to the Competent Authority along with the release approval.

9. Designated IT Wing

The following is the details for minimum resource to be part of IT Wing in PSWC for accomplishing various IT related tasks :

S.No.	Scope	Designation	Nos.	Purpose
1	Study Requirements / Change requests	Project Manager	1	- Study domain for news modules - Preparing SRS Documents - Providing domain knowledge to all resources - Testing of modules - Training to end users - Ensuring timely IT support to end users

2	Development – Web based	Sr. Software Developer / Software Developers	4	- Development of software modules as per SRS documents
3	Development of Mobile App	Mobile App Developer	1	- Development of Mobile App on Android and IOS platforms
4	Maintenance of Software modules	Software Developer	1	- Incorporation of changes as per approved change request
5	Database Maintenance	Database Administrator	1	- Regular tuning of database - Indexing as and when required - Ensure tables consistency - Necessary correction in data
6	Network Maintenance	Network Administrator	1	- Daily back up Database, Code, APIs and Reports - Tuning of Network - Maintenance of local server - Management

The resources shall be hired on outsourcing basis.

10. Official Communication / Correspondence

All in-house official correspondence / communication in PSWC shall happen through various electronics platforms introduced by IT Wing from time to time subject to the approval of Competent Authority. Video Conferencing shall be the primary platform for in-house meeting.

11. SOP for Software Modules

SOP for end users shall be prepared/revised with regards to use and compliance of all Software Modules, developed in-house / third party, implemented in PSWC.

12. Software Usage Policy

12.1 No other third-party software – free or licensed can be installed onto a computer system owned or provided to an employee by the organization, without prior approval of the IT Wing

12.2 Any software developed & copyrighted by the organization belongs to the organization. Any unauthorized use, storage, duplication or distribution of such software is illegal and subject to strict disciplinary action.

13. Critical Information Infrastructure

13.1 Critical Information Infrastructure (CII) is defined as “the computing & other resources, the incapacitation or destruction of which, shall have debilitating impact on security or safety of e-Governance application & databases of PSWC.”

13.2 The policy aims to identify the entire Information Communication Technology (ICT) Infrastructure at various locations being managed by the Corporation and declare Critical Infrastructure as Critical Information Infrastructure.

13.3 **Creation of Asset Register**

13.3.1 PSWC will create an asset register, a list of all the Information Communication Technology (ICT) infrastructure or related dependent infrastructure like hardware, networking resources, software resources (licenses and code), digital signatures, application software, digital data and backup assets which falls within the management scope of the respective office. (Refer Annexure F for sample format of asset register)

13.3.2 Every entry in asset register shall be assessed based on its functionality, criticality and sensitivity, degree of complementarities with other assets, degree of confidentiality based on strategic value and Time duration of availability. (Refer Annexure E for the description of the parameters)

13.3.3 The assessment shall assign confidentiality, Integrity and availability value collectively termed as CIA value (Refer Annexure F for sample format of asset register).

13.3.4 It is imperative to maintain asset register once it is created. There shall be a nodal officer to maintain asset register.

13.3.5 Half yearly or need based review of the asset register shall be conducted to keep track of changes.

13.3.6 Each asset assigned to any employee shall have proper receipts with signatures.

13.4 **Risk Analysis**

13.4.1 The PSWC shall conduct risk assessment of the assets in the asset register. A risk assessment is required to identify threats, human errors, malfunctioning virus attacks, vulnerabilities, Fire and their impact on assets by evaluating the probability of the occurrence of these threats/ vulnerabilities.

13.4.2 A risk analysis of the assets in asset register shall be done based on CIA rating. (Refer Annexure “G” for the sample risk analysis register).

13.4.3 Half yearly or need based review of the risk assessment shall be conducted to identify new risks and change the rating of existing risks.

13.4.4 PSWC will prepare a document containing the possible steps for mitigating such risks.

13.5 **Physical and Environmental Security**

13.5.1 PSWC shall safeguard the Critical Information Infrastructure against physical and environmental threats. Below are the key points to achieve Physical & Environmental Security.

13.5.2 The physical site shall be restricted for access to only authorized employees or designated users authorized by the Head of Department.

13.5.3 The Physical site and Data Center shall be monitored using Surveillance System like CCTV cameras. There shall be provision for 24*7 recording by the Surveillance System which shall be retained for at least one year.

13.5.4 The Physical Site shall be manned by deploying guards.

13.5.5 The Physical Site and Data Center shall have adequate systems provisioned for fire detection and safety.

13.5.6 The physical site & Data Centre shall have adequate systems, provision for detection of water leakage.

13.5.7 The physical site and Data Center shall have mechanism for detection of cooling issues.

13.5.8 The Data Center shall have adequate power supply control system like UPS, Gen Sets, etc.

13.6 Access Control to Critical Information Infrastructure

13.6.1 The PSWC shall identify and define access and its control procedures to Critical Information Infrastructure.

13.6.2 The PSWC shall maintain the access control in an access control matrix (refer to Annexure H for the sample of access control matrix).

13.6.3 The PSWC shall conduct half yearly or need based review of the access control matrix to add/delete accesses as per the changes in the organization structure to stop unauthorized people from accessing all or any component of related information of the Critical Information Infrastructure.

13.7 Business Continuity Plan

13.7.1 PSWC shall prepare a business continuity plan for un-interrupted availability of all key resources supporting business function. A business continuity plan shall include (Refer Annexure I for business continuity plan template)

13.7.2 Information of each Critical Information Infrastructure: This section includes list of all the declared Critical Information Infrastructure and their associated attributes like location, key stake holder(s) information, existing architecture, backup plan or reference to same.

13.7.3 Applicable scenarios for disaster declaration: This section lists the possible scenarios when arise warrant execution of specific corrective measures in order to maintain continuity of services. The list comprises of Natural, environmental, functional scenarios, human error & technological failure. All the scenarios shall list down specific procedures or reference to a disaster recovery plan to execute in case of declared disaster.

13.7.4 Communication Plan: This section defines the procedure to notify the disaster and details of mode of communication, content of communication, contact details of relevant stakeholders/response team and type of confirmation required to invoke disaster recovery.

13.7.5 Incident response team: This section defines the structure, roles & responsibilities, contact information of the response team whose members will execute the applicable disaster recovery plan as per point no 10.2. The structure shall clearly define the hierarchy and designation of the member.

13.7.6 Training, Testing & Exercising: This section defines the testing schedule, procedures, and forms for business recovery strategies and information technology recovery strategies along with the training plan of team members for business continuity.

13.8 Disaster Recovery Management (In case required)

13.8.1 PSWC shall prepare a disaster recovery plan for every Critical Information Infrastructure. A Disaster recovery plan shall be reviewed half yearly.
13.8.2 All disaster recovery plans will be part of business continuity plan and shall include:
13.8.3 Information of each failure point of associated Critical Information Infrastructure: This section includes details like function, location, key stake holder(s) information, existing architecture, backup plan or reference to same.
13.8.4 Communication Plan: This section defines the procedure to notify the disaster and details of mode of communication, content of communication, contact details of relevant stakeholders/response team and type of confirmation required to invoke disaster recovery.
13.8.5 Procedure to recover and resume operations: This section provides procedures or steps to recover and resume operations of the services offered by the associated Critical Information Infrastructure. Each step shall include the expected time taken.
13.8.6 Training, Testing & Exercising: This section defines the testing schedule, procedures, and forms for recovery strategies along with the training plan for team members.

13.9 Software & Critical Information Infrastructure Audit

An outsourced authorized State/Central Govt. empanelled agency shall be engaged for conducting annual software audit of all in-house developed software modules and Critical Information Infrastructure.

13.10 Software & Critical Information Infrastructure Audit Trail

Provision shall be incorporated in all the software modules and Critical Information Infrastructure for recording logs of all activities.

13.11 Backup Plan

13.11.1 PSWC shall create a back-up policy for applicable components of Critical Information Infrastructure. A backup policy shall include list of Components to be backed up, type of backup, backup frequency and backup retention and tool(s) used for backup.
13.11.2 Separate backup sets shall be maintained for weekly, monthly and yearly backup.
13.11.3 Logs of all backups shall be maintained for time period equivalent or grater then retention period of the backup.
13.11.4 There shall be provision to store a copy of backup at offsite secured location.(Refer Annexure J for Backup policy template)

13.12 Backup Policy

13.12.1 Backup policy allows to control what kind of backups are performed, how often data should be backed up, what software/hardware or cloud service should be used for performing backups, where backups are located, and who can access backups and how to contact them.
13.12.2 Daily complete backup shall be taken
13.12.3 Backup shall be taken using Veeam Backup
13.12.4 Backup is kept at data centre
13.12.5 Cloud Service Provider shall access it.

Details for Veeam Backup of all VM Servers on Cloud taken by Cloud Service Provider

Sr. No.	Backup	Schedule Interval	Backup Type	Retention Period
1	Complete Backup of Database Server	Daily 11.00 pm	Complete	One Month
2	Complete Backup of Application Server-1	Daily 11.00 pm	Complete	One Month
3	Complete Backup of Application Server-2	Daily 11.00 pm	Complete	One Month

13.13 Data Loss Prevention

PSWC shall provision necessary Infrastructure (IT and non-IT) to prevent data loss of the Critical Information Infrastructure. The deployed data loss prevention solution shall:

- Perform Identification, Authorization and Validation of all the data storage devices and access to the same.
- Provide secured storage inventory for all the data storage devices.
- Provision network monitoring tools for monitoring the unauthorized flow of data.
- Mandatory use of official email id for the transfer of data and any critical information.

13.14 Security

PSWC shall ensure deployment of procedures for protecting computers, networks, software and data from unauthorized access or damage.

14. Any Clarification or interpretation or amendment or addition in the policy shall be approved at the level of Managing Director, PSWC.

15. Amendment in the budget limit of IT hardware items mentioned in the policy as per latest market trend (if required) can be done at the level of Managing Director, PSWC.

Format-1

Request for Laptop by Branch Manager/District Manager/AAO

1.	Employee Code	
2.	Name of Officer	
3.	Date of Joining	
4.	Designation	
5.	Place of Posting	
6.	Date of Retirement	
7.	Bank Details	Name of Bank: Branch : A/c No. : IFSC :
8.	Whether any Desktop/ Laptop/ Tablet already issued. If Yes, whether the same has been returned back ?	

Declaration : I declare that I have not been issued any other official Desktop/Laptop/Tablet from any other State Department/ Board/ Corporation/ Society/ Commission/ any other state owned agency or Public Sector Undertaking.

Date : Signature of Officer

Approved By:

Annexure – A

DESKTOP		
S.No.	**Item**	**Minimum Specifications**
1.	**Processor**	Intel Core i5 (9th generation or higher) or equivalent
2.	**RAM**	4 GB upgradeable up to 16 GB or higher
3.	**Storage**	Minimum 500 GB or higher
4.	**Display**	17" LCD/LED or higher
5.	**USB**	Hi-Speed (USB 2.0) or higher
6.	**Network (RJ-45) Connector**	1000 BASE-T/100BASE-TX/10BASE-T x 1 or higher
7.	**Keyboard**	82 keys or higher
8.	**Operating System**	Mac OS or Microsoft Windows 10 Professional x64 or higher or equivalent

Annexure – A1

DESKTOP (All-in-One)		
S.No.	**Item**	**Minimum Specifications**
1.	**Processor**	Intel Core i7 (9th generation or higher) or equivalent
2.	**RAM**	8 GB upgradeable up to 32 GB or higher
3.	**Storage**	Minimum 500 GB or higher
4.	**Display**	23" LCD/LED or higher
5.	**USB**	Hi-Speed (USB 2.0) or higher
6.	**Network (RJ-45) Connector**	1000 BASE-T/100BASE-TX/10BASE-T x 1 or higher
7.	**Keyboard**	82 keys or higher
8.	**Operating System**	Mac OS or Microsoft Windows 10 Professional x64 or higher or equivalent

Annexure – B

LAPTOP		
S.No.	**Item**	**Minimum Specifications**
1.	**Processor**	Intel Core i5/i7 or equivalent processor.
2.	**RAM**	4 GB upgradeable up to 32 GB or higher
3.	**Storage**	Minimum 320 GB or higher
4.	**Display**	Minimum 13.3
5.	**USB**	Hi-Speed (USB 3.0) port type A Connector x 2
6.	**Network (RJ-45) Connector**	1000 BASE-T/100BASE-TX/10BASE-T x 1 or higher
7.	**Headphone**	Stereo, Mini Jack x 1 or more
8.	**Wi-Fi**	IEEE 802.11b/g/n, Maximum transmission speed: 300 Mbps*8, Maximum receipt speed: 300 Mbps*8
9.	**Integrated Web Camera**	Inbuilt web camera, 1.3 megapixels or higher
10.	**Keyboard**	82 keys or higher
11.	**Battery life**	Minimum 3 Hrs.
12.	**Operating System**	Mac OS or Windows 7 professional or higher or equivalent

Annexure – C

MULTI-FUNCTION PRINTER		
S.No.	**Item**	**Minimum Specifications**
1.	**Printer Type**	Laser
2.	**Memory Capacity**	128 MB
3.	**Paper Size**	A4, Letter and Legal
4.	**Print Speed**	Min 30 pages per minute for single side for A4
5.	**Model**	ADF
6.	**Interface**	- High Speed USB 2.0 - LAN (Optional) - Wireless LAN (Optional)

PRINTER		
S.No.	**Item**	**Minimum Specifications**
1.	**Printer Type**	Laser
2.	**Type of Printing**	Mono
3.	**Cartridge Technology**	Composite Cartridge
4.	**Memory Capacity**	128 MB
5.	**Paper Size**	A4, Letter and Legal
6.	**Print Speed**	Min 25 pages per minute for single side for A4
7.	**Number of Main Paper Tray**	One
8.	**USB Port**	Yes
9.	**Duplexing Feature**	Yes

Annexure – D

SCANNER		
S.No.	**Item**	**Minimum Specifications**
1.	**Scanner Type**	ADF (Automatic Document Feeder)
2.	**Scanning Modes**	Simplex / Duplex, Color / Grayscale / Monochrome
3.	**Document Size**	A4 and Legal
4.	**Print Speed**	Min 30 pages per minute for single side for A4
5.	**Scanning Speed**	Simplex = 20 ppm Duplex = 40 ppm
6.	**Interface**	USB 2.0
7.	**Supported OS**	Windows® 10 (32-bit/64-bit), Windows® 8.1/8 (32-bit/64-bit), Windows® 7 (32-bit/64-bit), Windows Vista® (32-bit/64-bit), Windows Server® 2016 (64-bit), Windows Server® 2012 R2 (64-bit), Windows Server® 2012 (64-bit), Windows Server® 2008 R2 (64-bit), Windows Server® 2008 (32-bit/64-bit), Linux (Ubuntu 16.04/14.04)

Annexure E

Functionality: This parameter identifies the functional capabilities of the Information system and its dependency upon the other Information systems of PSWC.

Criticality: This parameter identifies the relative degree of Criticality and sensitivity of Information Infrastructure Systems on the consequences of damage, lose, alteration and breach of confidentiality that impact the availability, accessibility, delivery and management of services offered by the Critical Information Infrastructure (CII). The more serious the consequences for the organization, the more sensitive and critical Information Infrastructure.

Degree of Complementarities: This parameter identifies the degree and type of sharing and linkage to the other Information Infrastructure Systems and provides the degree to which failure of one system can shut down affects other Critical Information Infrastructure relatively quickly in a cascading manner.

Time Duration: This parameter identifies the time duration of operation of Information Infrastructure as the same system may or may not be critical for all the time.

Annexure F: Sample Assets Registry Sheet

SNo	Asset Number	Asset Group	Description	Asset Quantity	C	I	A	CIA Total	Asset Value	Asset Classification	Location
Physical											
1	PSWC-S-01	Server	Server for Project	1	3	2	3	18	2	C4-Internal	<Location where the asset is installed>
Software Assets											
3	PSWC-O-01	System software	Application Software	6	1	2	3	6	1	C4-Internal	<Location where the asset is installed>
Services Assets											
4	PSWC-S-01	ILL	Internet Lease Line for Server and users	1	5	5	5	125	5	C1-Critical	

Description of columns:

B.1 Asset Number: In this field identification number of the asset will be written. Like for Server it can be unique asset no. etc. or department defined convention which can be easily identifiable.

B.2 Asset Group: In this field name, category of the assets will be written.

B.3 Description: Description of the asset will be written in this field.

B.4 Asset Quantity: In this field the actual quantity of the assets will be written.

B.5 'C' stand for Confidentiality (Access to authorized people): The value of this field will vary from 1 to 5, wherein

Value 1: Public/General: Information accessible to public requiring low security.
Value 2: All Employees: Information accessible to Persistent Systems employees and authorized non-Persistent Systems parties.
Value 3: Respective Functions: Information accessible to pre-approved group of people requiring moderate security.
Value 4: Need to Know - Restricted: Information accessible to pre-approved people and on need-to-know basis requiring high security.
Value 5: Very Sensitive - Critical: Information accessible to authorized people only requiring very high security.

B.6 'I' stand for Integrity (Safeguard accuracy and completeness of information): The value of this field will vary from 1 to 5, where in:

Value 1: Low: Information modified by unauthorized persons may lead to Business impact which is negligible.
Value 2: Medium: Information modified by unauthorized persons may lead to Business impact i which is noticeable.
Value 3: High: Information modified by unauthorized persons may lead to Business impact which is significant.
Value 4: Very High: Information modified by unauthorized persons may lead to Business impact which is serious
Value 5: Critical: Information modified by unauthorized persons may lead to Business impact which is disastrous and irreparable

B.7 'A' stand for Availability (Access to authorized people at right time): The value of this field will vary from 1 to 5, where in:

Value 1: < 35%: Downtime/unavailability which has very insignificant impact on business and operations.
Value 2: 35 to 70%: Downtime/unavailability, if exceeds 1 week, which has negligible impact on business and operations.
Value 3: 70 to 90%: Downtime/unavailability, if exceeds 1-3 business days, which has moderate impact on business and operations.
Value 4: 90 to 99.99%: Downtime/unavailability, if exceeds 8 hours, which has significant impact on business and operations.
Value 5: >=99.99%: Downtime/unavailability, if exceeds 4 hours, which has severe impact on business and operations.

B.8 CIA Total: This computation is the result of "C*I*A". Like if C = 3, I = 2 and A = 4, then CIA Total will be 3*2*4 = 24

B.9 Asset Value: This value also vary from 1 to 5, where in:

Value 1: CIA Total 0-6
Value 2: CIA Total 7-18
Value 3: CIA Total 19-27
Value 4: CIA Total 28-64
Value 5: CIA Total 65-125

B.10 Asset Classification

C1-Critical: Highest sensitive information which may lead to serious business impact. It requires a list of distribution to be maintained.
C2- Confidential: Sensitive business information, the unwanted disclosure of which can bring substantial financial damage, or damage to the company's reputation. It is information which can be of value to competitors. The information is shared between predefined and approved group of people.
C3- Restricted/Client Confidential: Sensitive information which may lead to breach of IPR. The information shared is between the clients and predefined and approved group of people within a project / function on Need-To-Know and Need-To-Use basis.
C4- Internal: Business information for which unwanted disclosure can have damaging consequences. This is generally information which is accessible to a wide circle of employees but is not intended for outsiders.
C5- Public: Information, which has been explicitly approved by the management for release to the public. This information is shared with the public outside Persistent Systems.

B.11 Location: In this field the exact location where the asset is located will be written.

Annexure G: Sample Risk Analysis Sheet

SNo.	Asset Number	Asset Name	Asset Value	Threats	Vulnerabilities	Impact	Likelihood	Risk Value	Controls & Safeguard	Likelihood after Controls	Residual Risk	Risk Status
Physical												
1	PSWC-S-01	Database	4	1. Accidental Loss of Data.	1.Lack of knowledge of the product	4	3	48	1. Access Control 2. Automated Weekly	1	16	Risk
People Assets												
2	Emp-876	Ram Kumar	3	Unplanned	Accidents, Ailments,	4	2	32	Backup Recourses	1	16	Risk

Description of columns:

C.1 Asset Number: In this field identification number of the asset will be written.

C.2 Asset Group: In this field name and category of the assets will be written.

C.3 Assets Value: This value will be copied from Asset Registry

C.4 Threats: Threats are the potential cause of an unwanted incident, which may result in harm to a system or department. "Asset Vulnerability Threat" populates threats associated with the respective vulnerability for respective information asset.

C.5 Vulnerabilities: Vulnerability is a weakness of an asset or group of assets that can be exploited by one or more threats. "Asset Vulnerability Threat" populates relevant vulnerabilities to the respective information asset by understanding controls in existence.

C.6 Impact: Rate the impact on business / function considering if Respective vulnerability is been exploited by associated threat. This impact would be in range of 1 to 5, where in:

Value 1: Low : Business impact which is negligible
Value 2: Medium: Business impact i which is noticeable
Value 3: High: Business impact which is significant
Value 4: Very High: Business impact which is serious
Value 5: Critical: Business impact which is disastrous and irreparable

C.7 Likelihood: Extent to which an event (Vulnerability exploitation by Threat) is likely to occur. This value may vary from 1 to 5, where in:

C.8 Risk Value: This field is computed based on the Asset Value, impact and Likelihood values entered. The computation is result of Asset Value * Impact * Likelihood. Priorities for risk mitigation are assigned based on the Risk Value.

Value 1: Rare Chance
Value 2: Low Possibility
Value 3: Medium Chance
Value 4: High Possibility
Value 5: Very High Possibility

C.9 Controls & Safeguards: List the Suggested controls/safeguards suggested for respective asset and identified vulnerability and threat.

C.10 Likelihood after Control: Extent to which an event (Vulnerability exploitation by Threat) is likely to occur after implementation of controls suggested by ISO27001:2005. The value may vary from 1 to 5, where in:

Value 1: Rare Chance
Value 2: Low Possibility
Value 3: Medium Chance
Value 4: High Possibility
Value 5: Very High Possibility

C.11 Residual Risk: This field is computed considering likelihood rating after control implementation. The formula for residual risk is Asset Value * Impact * Likelihood after Control Implementation Action.

C.12 Risk Status: This field is also computed and entered in the field. This value may vary from 1 to 5, where in,

Priority 1: Risk Value >= 50
Priority 2: Risk Value < 50 and >=40
Priority 3: Risk Value <40 and >=30
Priority 4: Risk Value <30 and >=20

Annexure H: Sample Access Control Matrix

		Authorization Levels on the various Applications				
SNo	**Resource Name**	**Sharepoint**	**ClearQuest**	**Test Machine**	**DB Servers**	**E-mail Alias**
1	Ram Kumar	Full Control/ Design/Rea	CCB-Assignee	Full Access	Full Access	Full Access
2	Sham Kumar	Design/Read/ Contribute	CCB-Assignee	No Access	No Access	No Access
3	Deepak Kumar	Design/Read/ Contribute	CCB-Assignee	No Access	No Access	No Access
4	Dheeraj Kumar	Design/Read/ Contribute	CCB-Assignee	No Access	Full Access	No Access

Annexure I: Sample Business Continuity Plan

1.0 Objective and Scope:

1.1 Objective

1.2 Scope

1.3 Assumptions

2.0 Critical Information Infrastructure:

Asset Name & description	Nodal Office Contact Information	Location	Stake holders Contact Information	Reference to Existing Architecture	Reference to Backup Plan	Reference to the Business continuity section under

3.0 Incident Response Team

3.1 Roles and responsibilities for team members:

3.2 Organization chart: Below is sample organization chart

3.3 Response Team Details

Member Name	Department/Designation	Email	Work Telephone	Home / Cell Telephone

3.4. Vendors & Contractors

Company	Contact Name	Emergency Telephone	Business Telephone

4.0 Business Continuity Strategies & Requirements

4.1. Asset Name:

4.1.1. Description:

4.1.2. Detailed procedures

4.1.3. Resource requirements

4.1.4. Logistics Support for execution of all recovery strategies

4.1.5. Data restoration plan for the recovery

4.1.6. Reference to disaster recovery plan.

5.0 Communication Plan

5.1 Incident detection and reporting

5.2 Alerting and notifications

5.3 Business continuity plan activation

5.4 Emergency operations centre activation

5.5 Damage assessment (coordination with emergency response plan) and situation analysis

5.6 Development and approval of an incident action plan

6.0 Training, Testing & Exercising

6.1 Training for business continuity team members

6.2 Testing schedule, procedures, and forms for business recovery strategies and information technology recovery strategies.

6.3 Schedule, triggers, and assignments for the periodic review of the business continuity and IT disaster recovery plan

6.4 Details of corrective action program to address deficiencies.

7.0 Business Continuity Plan Distribution & Access

7.1 The Plan will be distributed to members of the business continuity team and management. A master copy of the document shall be maintained by the business continuity team leader.

7.2 Provide print copies of this plan within the room designated as the emergency operations centre (EOC). Multiple copies shall be stored within the EOC to ensure that team members can quickly review roles, responsibilities, tasks, and reference information when the team is activated.

7.3 An electronic copy of this plan shall be stored on a secure and accessible website that would allow team member access if company servers are down.

7.4 Electronic copies shall also be stored on a secure USB flash drive for printing on demand.

Annexure J : Backup Policy Template

1.0 Purpose of the Policy

2.0 Scope

3.0 Procedure

4.0 Backup Content

5.0 Backup Types

Backup of servers will occur every day after regular business hours.

5.1 Full backup: Includes all the source files. This method ignores the file's archive bit until after the file is backed up. At the end of the job, all files that have been backed up have their archive bits turned off. Only one **full** backup will be done once a weekfollowed by **differential** and/or **incremental**.

5.2 Differential backups: Includes files that have been changed since the last Full (Clear Archive Bit) or Incremental backup. If the archive bit is on, the file is backed up, and archive bit is not turned off. The next time an incremental backup is done, this file is skipped (unless it is modified again).

5.3 Incremental backups: Includes only files that have changed since the last Full (Clear Archive Bit) or Incremental backup. The next time an incremental backup is done, this file is skipped (unless it is modified again).

6.0 Offsite Storage of Backup Media

Data Backup Template		
Date	Server	

Type of Backup Agent Needed

Windows	Version		Type	
Linux	Version		Type	
Unix	Version		Type	

List of Files and Folders to Backed Up

Backup Client and Policy

Backup Policy for Client Server:	☐F ☐D ☐I	**MON**	F ☐D ☐I	**TUE**	F ☐D ☐I	**WED**	F ☐D ☐I	**THU**	☐F ☐D ☐I	**FRI**	☐F ☐D ☐I	**SAT**	☐F ☐D I	**SUN**
Run Schedule for Policy:	AM:								PM:					

Only one Full (F) followed by either a Differential (D) or an Incremental (I)

Retention and Offsite

Retention Period of Backup	1	2	3	4
Offsite Storage				

Signatures

System/Backup/Administrator Signature	Date	