Draft Policy for Critical Information Infrastructure Of Punjab Government

Government of Punjab

Department of Governance Reforms,
SCO 193-195, Sector-34A,
Chandigarh-160022

Date of Issue : …….

1.0 Purpose to the Policy

This policy establishes guideline and procedures for identification of Critical Information Infrastructure (CII) across departments, corporations, boards and commissions of Government of Punjab.

2.0 Definitions

2.1. Critical Infrastructure: facilities, systems, or functions, whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of a nation and state.

2.2. Critical Information Infrastructure (CII): Information communication technology (ICT) infrastructure upon which core functionality of Critical Infrastructure is dependent. As per Section 70 of IT Act 2000, CII is defined as "the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety."

3.0 Objective of the Policy

3.1. To identify Critical Information Infrastructure (CII) in the Departments, Boards, Commissions, Corporations of Government of Punjab.

3.2. To declare identified Information Infrastructure as Critical Information Infrastructure under the Section 70 of the IT Act 2000.

3.3. To access threats, vulnerabilities and risk associated with Critical Information Infrastructure and their implication.

3.4. To provide measures for end to end protection to the Critical Information Infrastructure.

3.5. To provide the guidelines to implement disaster recovery and business continuity plan for Identified Critical Information Infrastructure assets.

4.0 Critical Information Infrastructure

4.1. Critical Information Infrastructure (CII) is defined as "the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety."

4.2. The policy aims to identify all the Information Communication Technology (ICT) Infrastructure being managed by the Department/Boards/Corporations/Commissions of Government of Punjab and declare Critical Infrastructure as Critical Information Infrastructure.

5.0 Identification of Critical Information Infrastructure

5.1. All the Departments, Boards, Commissions and Corporations shall identify the Critical Information Infrastructure within their infrastructure(s) on the basis of:

5.1.1. Functionality of the Information Infrastructure : refers to the functional capability of the Information system and its dependency upon the other Information system of Government of Punjab or Government of India

5.1.2. Criticality and Sensitivity: refers to the relative degree of Criticality and sensitivity of Information Infrastructure on the consequences of damage, lose, alteration and breach of confidentiality that impact the availability, accessibility, delivery and consumption of services offered by the Information Infrastructure. The more serious the consequences for the organisation, the more sensitive and critical Information Infrastructure.

5.1.3. Degree of complementarities with other information infrastructure in state and country: refers to the degree and type of sharing and linkage to the other Information Infrastructure and provides the degree to which failure of one system can shut down other Critical Information Infrastructure relatively quickly in a cascading manner.

5.1.4. Associated social, political, strategic values: refers to the importance of Information Infrastructure for political stability, economic prosperity, fraternity, unity and integrity of state and nation.

5.1.5. Time duration: refers to the time duration of operation of Information Infrastructure as the same system may or may not be critical for all the time.

5.2. The identification of critical infrastructure is a dynamic process and shall be reviewed half yearly to address changes in technologies and protocols.

6.0 Creation of Asset Register

6.1. The office(s) of Government of Punjab shall create an asset register, a list of all the Information Communication Technology (ICT) infrastructure or related dependent infrastructure like hardware resources, software resources (licenses and code), digital signatures, digital data and backup assets which falls within the management scope of the respective office. (Refer Annexure B for sample format of asset register)

6.2. 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 associated social, political and strategic value and Time duration of availability. (Refer Annexure A for the description of the parameters)

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

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

6.5. Half yearly review of the asset register shall be conducted to keep track of changes.

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

7.0 Risk Analysis

7.1. The office(s) of Government of Punjab shall conduct risk assessment of the assets in the asset register. A risk assessment is required to identify threats, vulnerabilities and their impact on assets by evaluating the probability of the occurrence of these threats/ vulnerabilities.

7.2. A risk analysis of the assets in asset register shall be done based on CIA rating. (Refer Annexure C for the sample risk analysis register).

7.3. Half yearly review of the risk assessment shall be conducted to identify new risks and change the rating of existing risks.

8.0 Physical and Environmental Security

8.1. All Departments, Boards, Corporations, and Commissions shall safeguard The Critical Information Infrastructure against physical and environmental threats. Below are the key points to achieve Physical & Environmental Security.

8.1.1. The physical site shall be restricted for access to only authorized employees or designated users authorized by the Head of Department. The access shall be controlled by the access control mechanism, like Smart cards, Biometric access etc. (refer section 9.0 of the policy for Access Control)

8.1.2. 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.

8.1.3. The Physical Site shall be manned by deploying guards.

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

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

8.2. Quarterly reviews and mock drills shall be conducted to check the credibility of the security system.

9.0 Access Control to Critical Information Infrastructure

9.1. The office shall identify and define access and its control procedures to Critical Information Infrastructure.

9.2. The office shall maintain the access control in an access control matrix (refer to Annexure D for the sample of access control matrix).

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

10.0 Business Continuity Plan

All Departments, Boards, Corporations, and Commissions shall prepare a business continuity plan for Critical Information Infrastructure(s). A business continuity plan shall include (Refer Annexure E for business continuity plan template)

10.1. **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.

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

10.3. **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.

10.4. **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.

10.5. **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 for business continuity team members.

11.0 Disaster Recovery Management

11.1. All Departments, Boards, Corporations, and Commissions shall prepare a disaster recovery plan for every Critical Information Infrastructure. A Disaster recovery plan shall be reviewed half yearly.

11.2. All disaster recovery plans will be part of business continuity plan and shall include:

11.2.1. 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.

11.2.2. 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.

11.2.3. 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.

11.2.4. Training, Testing & Exercising: This section defines the testing schedule, procedures, and forms for recovery strategies along with the training plan for team members.

12.0 Disaster Recovery Site

All the Departments, Boards, Commissions and Corporations shall maintain a Disaster Recovery Site preferably a central site for all Critical Information Infrastructure. There shall be half yearly review and audit and mock drills shall be

conducted at regular intervals preferably once every quarter. A Disaster Recovery Site shall:

12.1. Host the essential or minimum services to run the highly critical part of CII.

12.2. Have minimum impact of natural and environmental threats.

12.3. Have seamless connectivity with Data Center hosting Critical Information Infrastructure.

13.0 Backup Plan

13.1. All Departments, Boards, Corporations, and Commissions 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.

13.2. Separate backup sets shall be maintained for weekly, monthly and yearly backup.

13.3. Logs of all backups shall be maintained for time period equivalent or grater then retention period of the backup.

13.4. There shall be provision to store a copy of backup at offsite secured location.

(Refer Annexure F for Backup policy template)

14.0 Data Loss Prevention

14.1. All Departments, Boards, Corporations, and Commissions shall provision necessary Infrastructure (IT and non-IT) to prevent data loss of the Critical Information Infrastructure. The deployed data loss prevention solution shall:

14.1.1. Perform Identification, Authorization and Validation of all the data storage devices and access to the same.

14.1.2. Provide secured storage inventory for all the data storage devices.

14.1.3. Provision network monitoring tools for monitoring the unauthorized flow of data.

14.1.4. Mandatory use of official email id for the transfer of data and any critical information.

15.0 Interpretation & Modification of Policy

15.1. This Policy shall be valid for five years from the date of issuance of this policy.

15.2. Department of Governance Reforms reserves the right to bring any amendment, addendum, modification, revision etc. to this policy. Changes in the regulatory framework, technology, as well as market and technological advances may require revisions to this policy to keep the requirements and guidelines updated with the prevailing environment.

16.0 Effective Date:

16.1. This policy will be applicable with immediate effect.

17.0 Approval

17.1. This policy has been approved by the Council of Ministers as conveyed by the Department of General Administration Punjab vide their letter number < >, dated < >.

****

Annexure A

Functionality: The parameter identifies the functional capability of the Information system and its dependency upon the other Information system of Government of Punjab or Government of India.

Criticality: The parameter identifies the relative degree of Criticality and sensitivity of Information Infrastructure on the consequences of damage, lose, alteration and breach of confidentiality that impact the availability, accessibility, delivery and consumption of services offered by the Information Infrastructure. The more serious the consequences for the organisation, the more sensitive and critical Information Infrastructure.

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

Political, Economic, Social and Strategic Values: The parameter identifies the importance of Information Infrastructure for political stability, economic prosperity, fraternity, unity and integrity of state and nation.

Time Duration: The 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 B: Sample Assets Registry Sheet

SNo	Asset Number	Asset Group	Description	Asset Quantity	C	I	A	CIA Total	Asset Value	Asset Classification	Location
Physical											
1	DGR-S-01	Server	Server for Project	1	3	2	3	18	2	C4-Internal	<Location where the asset is installed>
Software Assets											
3	DGR-O-01	System software	Windows	6	1	2	3	6	1	C4-Internal	<Location where the asset is installed>
Services Assets											
4	DGR-S-01	VPN	VPN/Internet connectivity and email access	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 C: Sample Risk Analysis Sheet

SNo.	Asset Number	Asset Name	Asset Value	Threats	Vulnerabilities	Impact	Likelihood	Risk Value	Controls & Safeguards	Likelihood after Controls	Residual Risk	Risk Status
Physical												
1	DGR-S-01	Database Server	4	1. Accidental Loss of Data. 2. Hardware crashed.	1.Lack of knowledge of the product 2. Sudden power off.	4	3	48	1. Access Control 2. Automated Weekly Backups 3. Password Policy	1	16	Risk Mitigated
People Assets												
2	Emp-876	Ram Kumar	3	Unplanned	Accidents, Ailments, etc.	4	2	32	Backup Recourses	1	16	Risk Mitigated

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 D: 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/Read/ Contribute	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 E: Sample Business Continuity Plan

1.0 Objective and Scope:

1.1. Objective

1.2. Scope

1.3. Assumptions

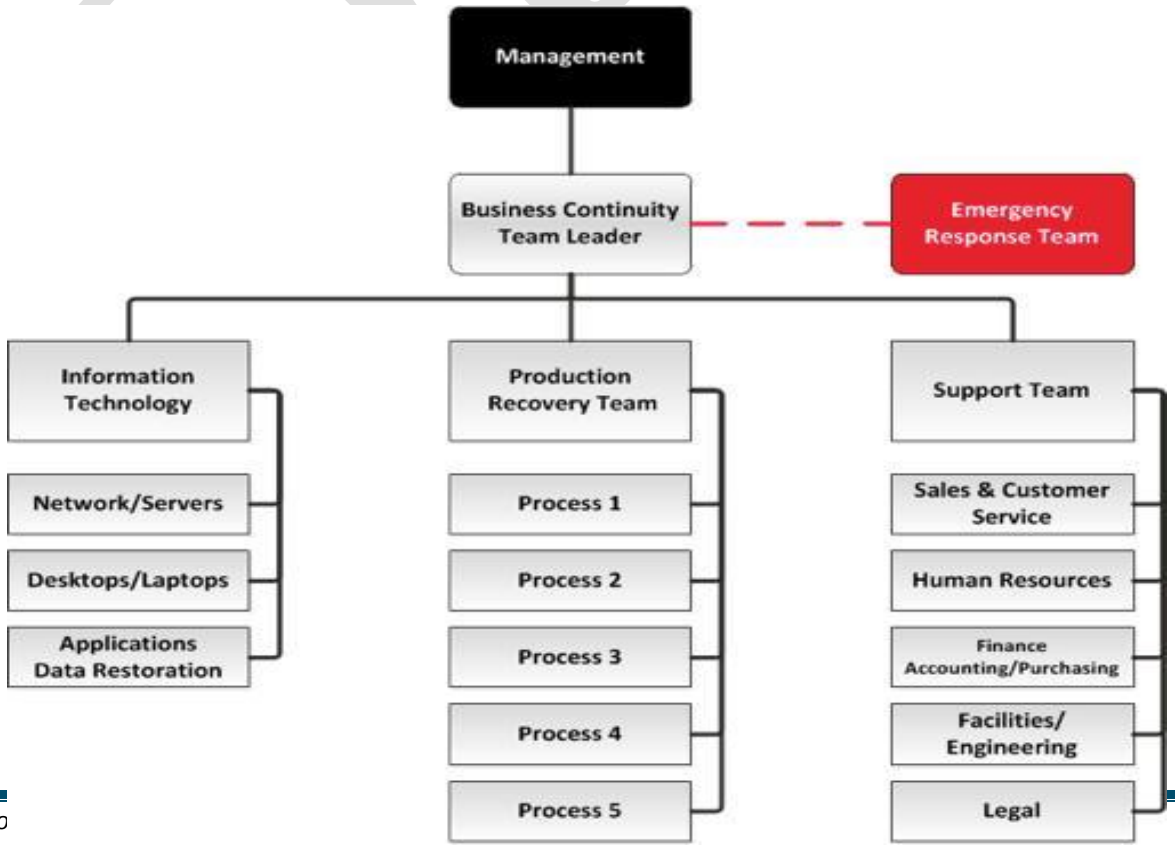
2.0 Critical Information Infrastructure:

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 point no 4.0

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 F: 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 week followed 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 tapes

Data Backup Template			
Date:		Server Name:	

Type of Backup Agent Needed

	Windows	Version:		Type:	
	Linux	Version:		Type:	
	Unix	Version:		Type:	

List of Files/Folders to be Backed Up

Backup Client and Policy

Backup Client Installed On Client Server:	☐ Yes										☐ No													
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 for Backup:	☐ 1 Week	☐ 2 Weeks	☐ 1 Month	☐ 2 Months
Offsite Storage:	☐ Yes		☐ No	

Signatures

Requestor's Signature:		Date:	
System/Backup Administrator Signature:		Date:	