



Application and Infrastructure Hosting Policy
for
Himachal Pradesh State Data Centre (HPSDC)

Department of Digital Technologies and Governance,
Government of Himachal Pradesh

1. Purpose

The purpose of this Policy is to establish guidelines and procedures for ensuring secure, reliable and efficient hosting of government applications and infrastructure in the Himachal Pradesh State Data Centre (HPSDC). This Policy has been designed based on the guidelines issued by the Indian Computer Emergency Response Team (CERT-In) of the Ministry of Electronics and Information Technology (MeitY), Government of India from time to time. The guidelines laid down in this Policy will be amended, as per advisories issued by CERT-In from time to time, keeping in view the emerging security threats and challenges which necessitate a change in the security posture of HPSDC.

2. Definition of Terms

- 2.1 **Cloud:** Refers to cloud computing, which is the delivery of various services (such as servers, storage, databases, networking, software, etc.) over the internet, allowing for scalable and flexible resource usage.
- 2.2 **Co-location:** A hosting option where organizations place their physical servers and other hardware in a data center and share the facility's resources, such as bandwidth, power, and cooling.
- 2.3 **CERT-In:** "Indian Computer Emergency Response Team (CERT-In)" has been established and appointed by Government of India as national agency in respect of cyber incidents and cyber security incidents in terms of the provisions of section 70B of Information Technology (IT) Act, 2000 (IT Act, 2000).
- 2.4 **DCO:** Data Centre Operator hired by the Department of Digital Technologies and Governance for the Operation and Management of Himachal Pradesh Data Centre
- 2.5 **Himachal Pradesh State Data Centre (SDC):** A centralized facility in the State which provides website/ application hosting, and security audit services to various government departments and organisations.
- 2.6 **Hosting:** The service of providing storage and compute resources to websites, applications, or data on a server.
- 2.7 **High Resource Requirement:** Refers to a virtual infrastructure required for an

application which is more than 8 vCPUs or 16 GB of RAM or 200 GB of storage.

2.8 **NDA:** Non-Disclosure Agreement

2.9 **Third Party Auditor (TPA):** A CERT-IN empaneled auditor engaged to conduct regular security audits of the HPSPDC and applications/ websites hosted in HPSPDC to ensure compliance with security standards and guidelines.

2.10 **VAPT:** Vulnerability Assessment & Penetration Testing (VAPT) is a security testing methodology in which the IT systems such as computers, networks and software such as operating systems and application software are scanned in order to identify the presence of known and unknown vulnerabilities.

2.11 **Vulnerability:** A weakness in a system or application that can be exploited by threats to gain unauthorized access to or perform unauthorized actions on the system.

2.12 **Virtual Private Server (VPS):** A virtual machine as a service, which runs its own copy of an operating system.

2.13 **Website:** A collection of related web pages located under a single domain name accessible through the internet.

2.14 **Web Application:** A web application is a computer program that utilizes web browsers and web technology to perform tasks over the Internet.

3. Government Guidelines regarding hosting of Government websites and applications

3.1 Cyber Security Guidelines issued by MeitY, GoI dated September, 2022 and Guidelines on Information Security Practices for Government Entities issued by CERT-In emphasizes government departments to:

"Ensure that the Applications/ websites/ services are hosted only at the designated data centers of Government or Cloud Service Providers empaneled by MeitY. No application/ website shall be hosted within the LAN segment of a Ministry/ Department/Office."

3.2 Government of Himachal Pradesh Office Manual 2011, Chapter XX also states that:

"The Departments must host their software applications/database etc. at the servers available in SDC or can co-locate their servers in the SDC, in consultation with DIT

HP. The departments must avoid replicating such infrastructure available at SDC. This will check proliferation of need to hire technical manpower for operation, administration and maintenance at departments and field offices."

- 3.3 Use of Himachal Pradesh State Data Centre service for hosting applications/ infrastructure:** All State Government Departments/ Boards/ Corporations/ Organizations are mandated to use State Data Centre services for hosting their official applications/ websites in HPSDC or co-locate their IT infrastructure in HPSDC. This shall be applicable for the new applications/ websites which shall be developed by the State Government Departments/ Boards/ Corporations and other Government organizations. For the legacy applications of State Government Departments which are not hosted on State Data Centre, migration period of maximum one year (from the date of notification of this policy) shall be allowed within which the concerned State Government Department/ Board/ Corporation shall get their legacy application migrated to HPSDC for hosting along with all legacy data.

4. HP State Data Centre

Himachal Pradesh State Data Centre (HPSDC) is one of the core ICT infrastructures established in the State, under National e-Governance Plan (NeGP) of Government of India, to consolidate services, applications and infrastructure, to provide efficient electronic delivery of G2G, G2C and G2B services. This is a common Data Centre created for use by different departments of the State Government. It hosts many mission critical applications/ infrastructures such as CCTNS, Excise and GST applications, eDistrict, Horticulture, Land Records, ICCC, CM Helpline, HPPCL etc. The HP State Data Centre facilitates hosting and management of various software applications online using common centralized system.

The HP State Data Centre was setup on 29th May, 2016. HPSDC is ISO 20000:2011 & 27001:2013 certified & all procedures in HPSDC have been framed as per ISO standards and CERT-IN guidelines issued by Government of India from time to time. A Third Part Auditor (TPA) has been engaged to conduct regular security audits of HPSDC. In addition to this, a Disaster Recovery site has been set up to keep backup of HPSDC data and applications at remote location.

Major benefits of HP SDC to user Departments/ Boards/ Corporations are as follows:

- a) Physical Security of Applications, Data and IT Infrastructure – Multiple layers of security along with surveillance mechanism.
- b) High Availability of services – Servers, Storage, Network and applications.
- c) Hosting is available on Virtual Private Server (VPS)/ Co-location/ sharing hosting model.
- d) Data Security through Firewalls, Intrusion Prevention System (IPS), Anti-DDoS, Web Application Firewall, Security information and event management (SIEM) tools and Endpoint security.
- e) Central Repository for Departmental Applications/ Data.
- f) 24×7 monitoring of servers, vendor support for faster resolution.
- g) Technical Support from HPSDC support team.
- h) Disaster Recovery (DR) for HPSDC and data is being replicated to the MeitY empaneled DR site.
- i) Dedicated Third Party Auditor for Security Audit/ Assessment and Service Levels monitoring.

5. Requisition by Government Departments/ Boards/ Corporations

5.1 The State Government Departments/ Boards/ Corporations shall place a requisition with the Department of Digital Technologies and Governance (DDTG), clearly specifying their status (Department, Board, or Corporation), the applications to be hosted in HPSDC along with resource requirement (CPU, RAM, Storage) & Operating System OR details of IT Infrastructure to be co-located in HPSDC.

The user department shall submit the required information along with the details of authorized signatory of the user Department who has the authority to submit duly signed and stamped change request form to HPSDC. All change requests related to the application/ infrastructure hosted in HPSDC shall be accepted only if the same are endorsed by the authorized signatory.

5.2 The Department of Digital Technologies and Governance (DDTG) shall scrutinize each application technically. It has been observed that many Government Departments/ Boards/ Corporations place requisitions for higher compute and storage resources (CPU, RAM, Storage) than the actual requirement. If upon scrutiny, it is observed that the requirement is excessive, the DDTG will advise the user Departments/ Boards/ Corporations accordingly.

6. Procedure for hosting Applications/ Infrastructure for Government Departments/ Boards/ Corporations

HPSDC hosting environment has two distinct zones, a staging area and production area. Staging area is an environment distinct from the production area, where all newly developed applications/infrastructure or changes in the existing applications are hosted for conducting security audit prior to hosting the same in the production area. No application/ infrastructure is allowed to be hosted directly in the production environment without undergoing security audit.

Once application is moved to the production area, after security audit, the same will be accessible to the end users through open internet. Any application submitted by the user department for hosting, is initially deployed in the staging area by the technical team of user department and ensure that it is functioning properly. The staging area has no internet access and hence application cannot be made live from the staging area. Once an application deployed in staging area, successfully audited by HPSPDC TPA, the same is deployed in the HPSPDC production area by Data Centre Operator.

The step-by-step procedure followed by the Data Centre Operator (DCO) to host departmental applications/ infrastructure in HPSPDC is as follows:

6.1.1 The Data Centre Operator of HPSPDC, after obtaining approval from DDTG for hosting a particular application in HPSPDC, will discuss the application requirements with concerned Government Department/ Board/ Corporation and then create the required environment in the staging area and initiate the security audit after successful application deployment.

6.1.2 Security audit of all departmental websites/ applications/ hardware is mandatory prior to hosting the same in HPSPDC.

- 6.1.3 Hosting of applications / infrastructure in HPSDC shall be allowed once the application/ infrastructure is security audited by the Third-Party Auditor and all vulnerabilities identified during the audit are required to be closed by the user department. Once the application / infrastructure is cleared by the TPA, the same will be allowed to be hosted/ co-located in the HPSDC.
- 6.1.4 If the department has already had its application security audited by another CERT-In empaneled security auditor, it will be permitted for hosting in HPSDC. The user department has to submit a copy of the security audit certificate, which must be no older than three months, along with the application hosting request form.
- 6.1.5 All mandatory documents/ forms for hosting (along with payment in case of Boards/ Corporations) must be submitted to DDTG prior to hosting the same in production environment of HPSDC. The list of prescribed forms, w.r.t. hosting of websites/ applications/ infrastructure in HPSDC, is given at Annexure-A.
- 6.1.6 If the application is web portal based and to be accessed through internet, a suitable domain name should either exist or be acquired by the user Department, e.g., "xxxx.hp.gov.in". For taking new URL under hp.gov.in domain, the department may submit requisition in writing to the DDTG.
- 6.1.7 Once application is hosted in HPSDC, it is regularly audited by the Third-Party Auditor appointed by DDTG and vulnerabilities, if any, found during the audit are shared with user departments for closure. The user departments are required to close the same in fifteen working days failing which, external access (through open internet) to such applications/ infrastructure would be stopped. The same may still be accessed through HIMSWAN network. However, after lapse of thirty working days, applications will be removed from production environment and infrastructure would be shut down permanently till the time all identified issues are resolved by the user Department. In case user department doesn't have requisite technical skills to rectify vulnerabilities, they may contact HPSEDC for the same on chargeable basis.
- 6.1.8 The user department is required to follow the standards and procedures laid down by the HPSDC, from time to time, for using its services. For example, HPSDC may close an application/ website that has not addressed the vulnerabilities, identified

during regular security audits, in the given time frame.

- 6.1.9 Any changes to the applications/ infrastructure hosted in HPSDC will be done in writing using change request forms. In case of any change, the application must undergo a security audit before deployment in the production environment of HPSDC.
- 6.1.10 No physical access to server farm area of HPSDC shall be provided to any user department personnel until and unless there is a justified reason submitted in writing with the approval of authorized signatory of the user Department.
- 6.1.11 No access to applications hosted in production environment of HPSDC from external network or internet shall be allowed for the purpose of installation/ upgrade/ backup of application / data etc. Users may access their applications in staging area and the same will be deployed to the HPSDC production environment by the Data Centre Operator.

7. Hosting Responsibilities

7.1 Responsibility Matrix for Application/ website Hosting at the SDC

Each activity shall have the involvement of multiple stakeholders. However, ownership of the same would differ and the roles of participating stakeholders shall be different, as defined below:

A – Advice (Advisory / Monitoring Role)

The Advisory role for any entity is such where the primary responsibility to execute the activity lies with someone else, and the advising entity is required to provide inputs and advice, whenever referred to by the primary stakeholder

E – Execute (Primary ownership)

Any entity responsible for executing any activity shall be the primary stakeholder for the same, and it is the said entity's responsibility to liaison with other stakeholders for coordination and inputs / advice for the execution & successful closure of the activity.



Application and Infrastructure Hosting Policy

C – Coordinate (Performing activities as directed / discussed)

The coordinating entity shall assist the primary stakeholder(s) (i.e., the activity executing entity) in successful execution of the tagged activity including performing various tasks for the completion as deemed required for the activity.

S No.	Activity	Stakeholders		
		User Department / Application Developer	DCO	DDTG
1	Application Design, Development, Testing and Release	E		
2	Infrastructure finalization for Application	E		A
3	Finalization of Infrastructure requirements at SDC	E	C	E
4	Application Hosting Testing in Staging Environment and Application Security Certification	E	C	C
5	Application Migration to SDC Live Environment	C	E	C
6	Application connectivity to SAN, and other common SDC Modules, and Web Connectivity (as applicable)	C	E	C
7	Performance and Health Monitoring	C	E	A
8	Error Reporting and Patch Management	E (Staging)	E (Helpdesk)	C
9	Ensuring Power, cooling, available common SDC security and Web & SWAN & SAN, connectivity, as applicable, to Application Servers		E	
10	Assessment of Application criticality for Disaster Recovery inclusion	E	C	E
11	Bring Application up at DR Site	E	C	C

12	Application resumption at HPSDC Site	E	C	
----	--------------------------------------	---	---	--

8. Co-Location Responsibilities

HPSDC Co-location Services offer a highly secure, environmentally conditioned and disaster resistant hosting space for the most optimum performance of customers' servers/ equipment. HPSDC Co-location Service is a service relationship between HPSDC and the user departments, in which customer's servers / equipment is housed in the facility of HPSDC. The User Departments shall use the infrastructure resources of HPSDC in an ethical and lawful manner for business purposes only.

8.1 HPSDC RESPONSIBILITIES

- 8.1.1 Co-located equipment would be governed by HPSDC information security policies so that they may not be insecure and pose a threat if placed along with HPSDC equipment, which, are governed by their Information Security requirements/ policies
- 8.1.2 Any End User Equipment used within HPSDC network for managing these shall be subject to HPSDC Information Security policies & procedures
- 8.1.3 HPSDC would be responsible for –
 - Availability of Rack Unit
 - Availability of UPS and Air conditioning
 - Availability of network and remote administration
 - 24x7 help desk
 - Availability of Close Circuit Camera
 - Providing physical access to User Departments after seeking the necessary approvals

8.2 USER DEPARTMENTS' RESPONSIBILITIES

Co-location service customers (User Departments) would be responsible for –

- 8.2.1 In Co-location service the User Departments assume all responsibilities, directly or

indirectly associated with their devices including their purchase, maintenance etc.

- 8.2.2 Co-location users have to seek prior permission for application generating high traffic or mails
- 8.2.3 Co-location system administrator will have to ensure application audit periodically as per the server and application audit policies mandated by DDTG
- 8.2.4 Co-location users would have to abide by the ISMS policies of HPSDC
- 8.2.5 While the equipment is located in the co-location facility the User Department is responsible for insuring, maintaining their equipment and providing cover against any risk of failure of the equipment
- 8.2.6 Co-location user will synchronize the clock with NTP server installed in HPSDC
- 8.2.7 Co-location users will follow the centralized policy for Antivirus management
- 8.2.8 Co-located system's administrators will have to ensure periodical patching of their OS/software/applications with latest updates from OEM/Manufacturer
- 8.2.9 Co-location users will allow HPSDC to monitor their services through Spectrum

9. Identity and Access Management

Any physical or logical access to HPSDC's 'Information Processing Systems' shall be controlled on the basis of business and security requirements.

9.1 User Access to Information, Data and Application:

- 9.1.1 HPSDC users shall be granted access to information, data and applications strictly on a "need to know" basis.
- 9.1.2 Access to information services shall be controlled through unique user ids, wherever possible, so that each user can be made accountable for their actions.
- 9.1.3 User access rights to applications and data shall be assigned only by the application administrator, on receipt of a documented approval from the designated authority, as well as from authorized personnel from Information Security Management

Forum (ISMF) or CISO. All access requests must include the purpose for request of access and nature of access

- 9.1.4 Application Administrator shall ensure that the level of access granted is appropriate to business requirements. Access should be confirmed from the application owner as well as custodian
- 9.1.5 If for any reason, a user's (user refers to system admin here) access rights need to be modified or revoked, the concerned designated authority must send an intimation of the same to the application administrator as well as Service desk. The application administrator shall then accordingly modify/ revoke the access rights after approval from the designated authority
- 9.1.6 Users will be required to re-authenticate themselves after a specific period of inactivity. All applications wherever possible shall use inactivity timeout as per the sensitivity of applications
- 9.1.7 All users shall be granted, "Read" access to all information classified as "public". Other rights to such information must be strictly reserved with the owner of such information

10. Payment modalities

- 10.1 As per the notification issued by this department dated 22.09.2021, government departments will not be charged for availing HP State Data Centre services, i.e., hosting of websites/ applications, co-location of hardware and security audit of websites/ applications/ infrastructure w.e.f. 1st October, 2021.
- 10.2 There shall be no charges for hosting applications/websites of Boards, Corporations, and other organizations within HPSDC until the requirements are cumulatively (for all applications/instances of the respective organization hosted in HPSDC) less than or equal to 8 vCPUs or 16 GB RAM or 200 GB Storage. For applications and services requiring infrastructure beyond these limits, and in the case of co-location, the charges for hosting will be governed by DDT&G letter number SITE-G-F07/5/2017-IT-Section-80 dated 17th May, 2017. There shall be no charge for Boards, Corporations, and other organizations for security audits of their websites/applications/infrastructure



hosted in HPSDC.

- 10.3 The invoice for the charges (if applicable) to the concerned Boards, Corporations, and other Organizations will be generated annually. In case of default on payment for more than 2 months, DDTG shall stop the access to the website/ application of the concerned organization.


**Approved vide NN-11 by
Chief Secretary to the
Government of Himachal Pradesh**

File No: E:208 SITE-F07/5/2017-IT SECTION — 109

Dated: 09.08.2024

Copy for information & necessary action is forwarded to: -

1. All the Administrative Secretaries to the Government of Himachal Pradesh.
2. All the Heads of the Departments in Himachal Pradesh.
3. The Registrar, HP High Court Shimla-171001.
4. The Divisional Commissioner, Shimla, Kangra and Mandi.
5. All the Deputy Commissioners in Himachal Pradesh.
6. All the Superintendent of Police in Himachal Pradesh.
7. All the Managing Director/ Member Secretary/ Commissioner / Secretary/ Chief Executive Officer/ Registrars of Boards/ Corporations/ Councils/ Authority/ Universities/ Municipal Corporations/ Co-Operative Banks in Himachal Pradesh.
8. Guard File


**Director,
Department of Digital Technologies and Governance,
Government of Himachal Pradesh**

Annexure-1

Sr. No.	Form Name	Request Form used for	HPSDC Form link on DDTG website
1	Application Details	Application details forms are used to collect specific information about application hosted in HPSDC.	https://ddtg.hp.gov.in/wp-content/uploads/2024/07/Application-details.pdf
2	Backup Form	Backup forms used to formalize and manage requests for data backup within an organization. Whether it's a full backup, incremental backup, or differential backup. How long the backup should be kept before it can be archived or deleted.	https://ddtg.hp.gov.in/wp-content/uploads/2024/07/HPSDC-FR-03-Ver-1.4-Backup_form.pdf
3	Change Management Form	The form initiates the change management process by detailing the proposed change, its rationale, scope, potential impact, and required resources.	https://ddtg.hp.gov.in/wp-content/uploads/2024/07/HPSDC-FR-04-Ver-1.4-ChangeManagement.pdf
4	Domain User Creation/ Deletion Form	Domain user creation and deletion request forms are used in IT and administrative settings to manage the provisioning and deprovisioning of user accounts within a domain or network	https://ddtg.hp.gov.in/wp-content/uploads/2024/07/HPSDC-FR-05-Ver-1.5-Domain-user-Creation_Deletionform.pdf
5	Data Restore	The Data Restore Request Form is used by organizations to facilitate the recovery of lost or corrupted data from backups. This form helps streamline the process of restoring data while ensuring that necessary information and approvals are documented	https://ddtg.hp.gov.in/wp-content/uploads/2024/07/HPSDC-FR-06-Ver-1.4-Data-Restore.pdf
6	Firewall Change Management Form	The Firewall Change Management Request Form is a structured document used by IT departments and network administrators to manage and document changes to firewall configurations. These forms are crucial for maintaining	https://ddtg.hp.gov.in/wp-content/uploads/2024/07/HPSDC-FR-07-Ver-1.4-Firewall-Change-Mgmt-form.pdf

Application and Infrastructure Hosting Policy

		network security, ensuring compliance with policies, and minimizing risks associated with unauthorized or incorrect changes	
7	Network Configuration Change Management	Network Configuration Change Management Request Forms are crucial documents used by IT departments to manage and document changes to network configurations. These forms help ensure that network changes are implemented in a controlled and systematic manner, minimizing disruptions and maintaining network integrity.	https://ddtg.hp.gov.in/wp-content/uploads/2024/07/HPSDC-FR-08-Ver-1.3-Network-Config-Change-Management.pdf
8	Password Reset & Change	Password Reset and Change Request Forms are used for need to reset their passwords or change their existing passwords. These forms help streamline the process and ensure that password-related requests are handled securely and efficiently.	https://ddtg.hp.gov.in/wp-content/uploads/2024/07/HPSDC-FR-09-Ver-1.3-Password-Reset-Change.pdf
9	VPN Request Form	The VPN Request Form is used by organizations to manage requests from employees or authorized users who need access to the organization's network resources via Virtual Private Network (VPN). VPNs are crucial for secure remote access to internal systems, especially when employees work remotely or need access while traveling.	https://ddtg.hp.gov.in/wp-content/uploads/2024/07/HPSDC-FR-11-Ver-1.4-VPN-Request-form.pdf
10	DNS Creation/ Modification/ Deletion Form	The VPN Request Form is used by organizations to manage requests from employees or authorized users who need access to the organization's network resources via Virtual Private Network (VPN). VPNs are crucial for secure remote access to internal systems, especially when employees	https://ddtg.hp.gov.in/wp-content/uploads/2024/07/HPSDC-FR-25-Ver-1.4-DNS-Creation_Modification_Deletion-form.pdf

		work remotely or need access while traveling.	
11	Public IP Request Form	The Public IP Request Form is used by organizations to manage and document requests for public IP addresses. These forms are typically used when an organization needs to assign a public IP address to a specific device, server, or service that requires direct access from the internet.	https://ddtg.hp.gov.in/wp-content/uploads/2024/07/HPSDC-FR-26-Ver-1.4-Public-IP-Request-Form.pdf
12	SAN Request Form	The SAN (Storage Area Network) Request Form is used by organizations to manage and document requests for storage resources in their SAN infrastructure. SANs are specialized networks designed to provide access to consolidated, block-level data storage. These forms ensure that requests for SAN resources are processed securely, approved by appropriate stakeholders, and aligned with organizational storage policies and requirements.	https://ddtg.hp.gov.in/wp-content/uploads/2024/07/HPSDC-FR-27-Ver-1.4-SAN-Request-Form.pdf
13	Website Hosting Request Form for Production Environment	The Website Hosting Request Form for Production Environment" is a structured document used by organizations to manage and document requests for hosting new websites or web applications in their production environment. This form helps ensure that hosting requests are processed securely, approved by appropriate stakeholders, and aligned with organizational standards and security policies	https://ddtg.hp.gov.in/wp-content/uploads/2024/07/HPSDC-FR-28-Ver-1.4-Website-Hosting-Request-Form-for-Production-Environment.pdf

14	Private IP Request Form	The Private IP Request Form is used by organizations to manage and document requests for private IP addresses within their internal network infrastructure. Private IP addresses are used for internal communication within a network and are not routable over the internet. These forms ensure that requests for private IP addresses are processed securely, approved by appropriate personnel, and aligned with organizational network policies.	https://ddtg.hp.gov.in/wp-content/uploads/2024/07/HPSDC-FR-29-Ver-1.4-Private-IP-Request-Form.pdf
15	Website Hosting Request Form in Staging server	The Website Hosting Request Form for Staging Server is used by organizations to manage and document requests for hosting websites or web applications in a staging environment. Staging environments are used for testing, quality assurance (QA), and pre-production activities before deployment to the live or production environment. These forms ensure that hosting requests for staging servers are processed securely, approved by appropriate stakeholders, and aligned with organizational standards and deployment processes.	https://ddtg.hp.gov.in/wp-content/uploads/2024/07/HPSDC-FR-30-Ver-1.3-Website-Hosting-Request-Form-in-Staging-server.pdf
16	Hardware Hosting Request Form in Staging room	The Hardware Hosting Request Form for Staging Room is used by organizations to manage and document requests for hosting hardware equipment in a staging or testing room environment. Staging rooms are dedicated spaces where hardware setups, configurations, and testing activities are conducted before deployment to production or operational	https://ddtg.hp.gov.in/wp-content/uploads/2024/07/HPSDC-FR-31-Ver-1.4-Hardware-Hosting-Request-Form-in-Staging-room.pdf

		environments. These forms ensure that requests for staging room resources are processed securely, approved by appropriate stakeholders, and aligned with organizational standards and deployment processes	
17	Authorized Persons Request Form	An Authorized Persons Request Form is used by organizations to manage and document requests for authorizing individuals or entities to perform specific actions or access certain resources within the organization. These forms help ensure that access permissions are granted appropriately, in line with organizational policies and security protocols	https://ddtg.hp.gov.in/wp-content/uploads/2024/07/HPSDC-FR-36-Ver-1.1-Authorized-Persons-Request-Form.pdf
18	Data Deletion	The Data Deletion Request Form is used by organizations to manage and document requests from individuals or entities to delete specific data or information held by the organization. This form ensures that data deletion requests are handled securely, in accordance with applicable data protection regulations (such as GDPR, CCPA), and organizational policies	https://ddtg.hp.gov.in/wp-content/uploads/2024/07/HPSDC-FR-37-Ver-1.1-Data-Deletion.pdf
19	Hardware Hosting Request Form in Production Environment	The Hardware Hosting Request Form for Production Environment is used by organizations to manage and document requests for hosting hardware equipment in a production environment. Unlike staging or testing environments, production environments are live systems where operational processes and critical applications run.	https://ddtg.hp.gov.in/wp-content/uploads/2024/07/HPSDC-FR-39-Ver-1.3-Hardware-Hosting-Request-Form-in-Production-Environment.pdf

20	Material Movement Form-3	The Material Movement Request Form is used by organizations to manage and document requests related to the movement of materials or goods within a facility or between different locations. These forms ensure that material movements are tracked, authorized, and conducted efficiently while maintaining inventory accuracy and operational control	https://ddtg.hp.gov.in/wp-content/uploads/2024/07/HPSDC-FR-41-Ver-1.2-Material-Movement-Form.pdf
21	VM Creation Request Form	The VM Creation Request Form is used by organizations to manage and document requests for creating Virtual Machines (VMs) within their IT infrastructure. These forms ensure that VM deployments are handled efficiently, in accordance with organizational policies, and to meet specific business needs.	https://ddtg.hp.gov.in/wp-content/uploads/2024/07/HPSDC-FR-43-Ver-1.1-VM-Creation-Request-Form.pdf

