सत्यमेव जयते

Digital India
Power To Empower

NIC

CORE SERVICES

HANDBOOK

About the Handbook

NIC delivers core IT Services to the Government at the centre States and district. By providing the network backbone and e-Governance support to Central Government, State Governments, UT Administrations, Districts and other Government bodies, NIC is enabling a more efficient and participative Government. NIC is at the core of the eGovernance framework and empowering the Digital India initiative as it offers a wide range of ICT services.

At NIC we endeavour to ensure that the latest technology in all areas of IT is available to its users. We provide end-to-end solutions to the Government and are actively involved in all IT enabled applications and have empowered the Government officials to make use of the latest digital technology in their day to day activities to provide better services to the citizens.

This handbook provides a brief overview of all core services offered by NIC , including a single portal for on-boarding process and complaint registration. Services like Application Security, Email, SMS, Domain registration, VPN, Video conferencing, Wi-fi etc are part of this handbook.

NIC Core services collectively support the entire governance framework under Digital India. Supported by a network of skilled engineers, and a rapid response to any complaint through the 24x7 service desk, these services ensure dependable, redundant and comprehensive ICT support to the Government.

Table of Content

1. Application Security Compliance..... 3
2. Authentication services..... 5
3. Cloud services..... 6
4. Domain Name System (DNS)..... 8
5. E-Mail Services..... 9
6. e-Sampark..... 12
7. End-point security..... 14
8. e-Sign Service..... 16
9. Firewall Access Rule Processing System (FARPS)..... 18
10. Gov. in Registration..... 20
11. SMS Gateway..... 23
12. Virtual Private Network..... 25
13. Video Conferencing..... 28
14. Vulnerability Assessment..... 29
15. Web Application Firewall (WAF)..... 31
16. Webcast..... 33
17. Wi-Fi..... 35

Annexure 1 36

(Single Window for Registration of NIC core Services – eForms).....

Annexure 2..... 37

Service Desk).....

1. Application Security Compliance

A. About

Application security compliance involves providing independent evaluations of applications based on security policies, procedures, standards, measures and practices for safeguarding application's information from loss, damage, un-intended disclosure, or denial of service etc. Due to emerging cyber security threat, Application Security compliance becomes most important.

As per Application Security Audit policy of NIC (Cyber Security Policies, Guidelines and Procedures for NIC Information Infrastructure) , it is mandatory for all websites / applications hosted at the NIC data centres to go through a complete security audit process before they can be on-boarded or whenever an alteration/addition is made to the application.

There are two services offered under application security compliance:

a. **Application Security Audit Services:**

   Security audit of applications is carried out in-house by Application security group as per requests for audit.

b. **Penetration Testing Services:**

   Random penetration testing is performed by Application security group and aimed at enhancing the application infrastructure security with a continuous assessment for security provisioning of hosted applications and their environment. User is required to close the vulnerabilities identified during the testing.

B. Eligibility to Avail Service

All applications hosted in the NIC data centre are required to go through audit process and security audit clearance from Application Security Group (ASG).

C. How to register for the service

A single window platform is available for seamless registration of all NIC services, refer **Annexure 1** for more details on online forms.

D. Guidelines

a. Application Security Infrastructure Audit Services:

For details of the audit process refer
https://security.nic.in/Audit_Process.aspx

b. Penetration Testing Services:

Vulnerabilities found during the penetration testing are reported to the user through ticking system, and the user can view/respond to the ticket, using the link at: http://asts.nic.in/scp

E. Complaint Registration

A user friendly service desk portal is available to register complaints related to all services. Refer Annexure 2 for more details.

2. Authentication services

A. About

Authentication services offer ease of user access and gives a single source of authentication to various applications thereby ensuring that a user can use a single user ID and password to access a plethora of Government portals. Secure Light Weight Directory Access Protocol (SLDAP) is used to provide secure authentication to all the applications integrated with the central LDAP server of NIC. This is one of the services offered under Messaging services of NIC and over 400 applications are integrated to authenticate their users.

B. Eligibility to Avail Service

- Any applications hosted on NICNET & NIC Data Centre's.
- User should have a @gov.in/@nic.in user ID.

The pre-requisites are as mentioned below:

a. The application should have security audit clearance from the Cyber security Division of NIC or a Cert-In empanelled vendor.

b. The application should be accessible over HTTPS only.

C. How to register the service

A single window platform is available for seamless registration of all NIC services, refer **Annexure 1** for more details on online forms.

D. Complaint Registration

A user friendly service desk portal is available to register complaints related to all services. Refer Annexure 2 for more details.

3. Cloud services

A. About

To accelerate the delivery of convenient e-Services to citizens from the Government, there was a need to offer Cloud Computing Services from Data Centers, for this NIC launched National Cloud in year 2014 under the umbrella of MeghRaj, Government of India Cloud Initiative of MeitY. NIC National Cloud service offerings include IaaS (Infrastructure as a Service), PaaS (Platform as a Service), etc. for scalable ICT infrastructure for quick deployment of e-Governance initiatives of the Government. Cloud services ensure standardization, interoperability, integration and pooling of scarce resources for provisioning of cost effective and agile services for rapid implementation of e-Governance initiatives of Government.

National Cloud Services is providing hosting support on 24x7 Basis for various critical e-Governance Projects viz. Aadhaar Enabled Biometric Attendance System (AEBAS), Swachh Bharat Mission, National Portal of India, Jeevan Pramaan, CCBS, NREGA, MyGOV, Digital Locker, JoSSA& NEET(Counselling), ORS(e-Hospital), National Scholarship, e-NAM, mFMS, GeM, Cyber Swachhta Kendra, Digital India Portal, National Transport Project, ShramSuvidha Portal, Prime Minister Office website, eNAM, Govt. Websites etc.

Since the launch of National Cloud Services, there has been exponential demand for Cloud keeping in view the cloud first policy of MeitY. To cater to increased demand of Cloud for e-Governance Services, National Cloud was further enhanced to provide services from multiple locations of NDC Hyderabad and Pune.

B. Eligibility to Avail Service

- All applications under Government both at the Centre and State
- This service is offered to users having @gov.in/@nic.in email id.

C. How to register for the service:

A single window platform is available for seamless registration of all NIC services, refer **Annexure 1** for more details on online forms.

D. Guidelines

For further details refer to https://cloud.gov.in/onboarding_procedure.php

E. Complaint Registration

A user friendly service desk portal is available to register complaints related to all services. Refer Annexure 2 for more details.

F. Additional Information

Users under payment/chargeable category will have to take cloud resources through NICSI.

4. Domain Name System (DNS)

A. About

The Domain Name System (DNS) is a hierarchical, distributed database. It stores information for mapping Internet host names to IP addresses and vice versa, mail routing information, and other data used by Internet applications. Clients look up information in the DNS by calling a resolver library, which sends queries to one or more name servers and interprets the responses. NIC is managing numbers of authoritative and recursive DNS servers which are placed at geographically different locations in the country to maintain redundancy, high availability and minimize latency. NIC has categorized DNS servers according to domain names.

NIC also maintains DNS record for domains other than nic.in and gov.in like .in, org.in, res.in, ac.in etc. Domains should be registered with designated Registrar for this purpose.

B. Eligibility to Avail Service

- This service is offered to domains which are hosted on NICNET IPs.
- Registration under Domain name NIC.IN is restricted to organizations/ministries under state/central Govt., autonomous bodies under central/state Govt. and Public sectors under state/central Govt.

C. How to register for the service

A single window platform is available for seamless registration of all NIC services, refer **Annexure 1** for more details on online forms.

D. Complaint Registration

A user friendly service desk portal is available to register complaints related to all services. Refer Annexure 2 for more details.

5. E-Mail Services

A. About

Email services offered by NIC have been in operation for over a decade and a half in different models. In Feb 2015, the Government issued the **"Email policy of the Government"** that mandates all Government officials, both at the centre and state to use only Government Email service for official correspondence and have the address as **@gov.in.** The implementing agency for the policy is NIC.

The primary trigger behind the policy was security of Government data which resides on servers outside India and on servers beyond the control of the Government of India.

Highlights:

- Government officers who resign or superannuate after rendering at least 20 years of service shall be allowed to retain the name based e-mail address i.e. **userid@gov.in** for one year post resignation or superan nuation. Subsequently, a new e-mail address with the same user id but with a different domain address for instance i.e. **userid@pension.gov.in**, would be provided by NIC. During the one year users should inform all concerned regarding the change of address. User can retain the same login id and password for access.
- Intimation to NIC HQ Messaging Division by NIC coordinators in Ministries & Departments/ SIO's/DIO's with details of officials retiring in their respective areas is mandatory for service continuity.
- Based on the request of the respective organizations, two ids can be created for an officer, one based on the designation and the other based on the name of the officer.
- The service allows registration of virtual domains representing the Ministry/Department. For instance **userid@meity.gov.in**, **userid@mea.gov.in** etc.

The email is as per global standards having enhanced features like briefcase, dumpster, calendar, threaded view etc. and security features like geo fencing, and secure device access.

The service ensures security, performance, availability, redundancy and service continuity in addition to a rich feature set.For security, Mobile number registration is a mandatory requirement for the Government email ID. All alerts will be sent to the registered number.

B. Value added Services under Messaging:

1. **IMAP/POP: Government email can be configured on all devices that includes phone, laptops, iPads etc.** However, for security**,** by default NIC email service is available over web only. If a user wants to access the service through IMAP/POP, he has to register for the same.
2. **Distribution List Service:** This provides group e-mail services and SMS lists known as the "Distribution list". Various Ministries and Departments including NIC, use this facility to broadcast official e-mails and SMS to their members within their respective departments/ Ministries. As of today more than 2000 distribution lists have been made available. Mission critical lists like sio-list, hod-list, hog-list are moderated and maintained by the Messaging division. Refer guidelines under "Ë" below.
3. **SMTP Gateway Service:** This is a platform for applications to send bulk e-mails or notification emails from their portals. Applications hosted in NIC data centres can be integrated with this platform to send emails to their users.
4. **Authentication Service:** Authentication services have been offered for ease of user authentication and gives a single source of authentication to various applications. For more details refer service mentioned under point no. 2 in the index.

5. **Reset Forgotten Password**: If a user has forgotten the password, using this service, user can change or reset the password without the need to call up the complaint desk.

i. Pre-requisite to access the service:

- User's current mobile number must be updated in NIC LDAP as OTP is sent to the registered mobile number.
- Link of the portal: **https://passapp.emailgov.in**

6. Logapp Service: This service allows users to see the "LAST LOGIN details along with Password Change History" for his/her account (email id) for the past one month. It helps users remain updated about his/her account, thereby ensuring that s/he take corrective action in time to prevent unauthorized access to his/her email account. This service sends SMS alerts in case unauthorised access is observed. Link of the portal:

https://logapp.emailgov.in

C. Eligibility to Avail Service

This service is offered to all government officials from central or state departments free of cost and to PSUs under paid category through NICSI.

D. How to register for the services

A single window platform is available for seamless registration of all NIC services, refer **Annexure 1** for more details on online forms.

E. Guidelines

- Refer **https://msgapp.email.in/docs/**for more details of email policy and e-mail account management.
- Refer **https://msgapp.emailgov.in/docs/**for Distribution list policy.

F. Complaint Registration

A user friendly service desk portal is available to register complaints related to all services. Refer Annexure 2 for more details.

6. e-Sampark

A. About

e-Sampark was introduced as a part of early harvest program under Digital India Initiative to establish proactive communication by digitization of campaigns/ SMS sent out to citizens/elected representatives. e-Sampark reduces the gap between government Ministries/Departments by sending the recent updates/policies directly to the citizens through email /SMS thus incorporating communication by digitization.

Using the Sampark database the Government can reach out to people individually or in groups/ sets of users depending on the requirement. Information, alerts, feedback for a programme, policy drafts etc. can be sent to a targeted user base thereby improving the efficiency of governance and e-Governance efforts.

The Sampark database includes email and mobile numbers of Government officials, elected representatives and citizens as per their profession. Central and State Government can leverage this platform to send information and take feedback about their policies and initiatives in **English/ Hindi or any of the regional language** thus increasing the impact of their endeavour. This database is regularly augmented with email address and mobile numbers. As of today the database of e-Sampark with valid email addresses is **over 3.32 Crore** and a **validated mobile number** count of **over 96.20 Crore**. This mobile database is segregated based on **telecom circle wise and state wise** for high impact of campaigns.

Using the Sampark Intranet site https://sampark.nic.in (accessible from NICNET/VPN) Nodal officers of each Ministry and department both at the centre and State can upload their data to the sampark Db for their respective Ministry/Department, view/ADD/update data, send/schedule bulk email/SMS campaigns, Search facility for searching employees based on

name, email, mobile etc.

Till date700+ Mail campaigns and over 670 Cr SMS have been sent. All major initiatives of the Govt including MyGov, Hon'ble PM's **Mann Ki Baat, BHIM, etc.** have leveraged this platform of their campaigns.

B. Eligibility to Avail Service

This service is offered to Ministries/Departments and States across all tiers of the Government framework– including Central Government, State / UT Governments and local bodies.

Mailers under eSampark are not charged, however SMS sent under e-Sampark is a paid service through NICSI.

C. How to register for the service

A single window platform is available for seamless registration of all NIC services, refer **Annexure 1** for more details on online forms.

Citizens can subscribe to e-Sampark by giving missed call, or by sending SMS or the through e-Sampark website.

D. Guidelines

I. Referhttps://sampark.gov.in/sampark/ for more details.

ii. Best Practices for designing an mailer

https://sampark.gov.in/Sampark/guidelines/tips-designing.html

iii. Tips for creating an effective mailer

https://sampark.gov.in/Sampark/guidelines/tips-effective.html

iv. Mailer dissemination Guidelines

https://sampark.gov.in/Sampark/guidelines/tips-request.html

E. Complaint Registration

A user friendly service desk portal is available to register complaints related to all services. Refer Annexure 2 for more details.

7. End-point security

A. About

NIC has deployed centrally managed antivirus solutions from three different OEMs in NICNET, namely, Trend Micro, Symantec and McAfee. All the States and various Bhawans / Ministries / Departments in Delhi are given one solution out of the above three solutions to protect the systems from viruses, worms, Trojans, bots, ransomware and other malwares.

Besides providing the centrally managed Antivirus Service, NIC has deployed centrally managed patch management solutions, namely, IBM's Tivoli Endpoint Manager and Microsoft SCCM (System Centric Configuration Manager). In addition to these two solutions, for the updation of software patches, Microsoft's WSUS (Windows Server Update Service) is also deployed in various States all over the country and Bhavans in Delhi. These solutions are used to patch the vulnerabilities in OS and other applications running on the systems so that attackers are not able to compromise the systems in NICNET.

An in-house application SARS (Security Alerting and Reporting System), hosted at **https://soc.nic.in** has been developed to monitor the antivirus status and for various other security related reports. The SARS portal may be accessed using NIC email user-id's by the authorised network administrators of the Bhavans and NIC State Centres.

The logs pertaining to the network activity of the client systems is monitored by the Cyber Security team on 24x7 basis. Based on this, any malicious/unauthorized activity performed by the client systems is detected and alert mail is sent to the concerned Network Administrator and HOD/SIO.

Timely action of the concerned Network Administrator is essential to avoid further spread of malware on other systems in the network.

B. Eligibility to Avail Service

The Endpoint Security service is offered to various Government Ministries and Departments by NIC on the recommendation of concerning HoD / HoG / SIO and approval of the competent authority for NICNET connectivity and provisioning of the Endpoint Security service. The service can be availed, subject to the availability of required licenses for Endpoint Security solutions.

C. How to register for the service

- A single window platform is available for seamless registration of all NIC services, refer **Annexure 1** for more details on online forms.
- On submission of the approval to Network Security Division, the Endpoint Security service is provisioned. For communication during deployment and help during post-deployment, the user may contact at antivirus@nic.in.

D. Complaint Registration

A user friendly service desk portal is available to register complaints related to all services. Refer Annexure 2 for more details.

8. e-Sign Service

A. About

e-Sign is an integrated service that facilitates issuance of Digital Signature Certificate and signing of requested data by authenticating AADHAAR holder. It facilitates electronically signing a document by an Aadhaar holder using an online service. Aadhaar id is mandatory for availing e-Sign Service. It is designed for applying Digital Signature on the document using Aadhaar KYC service for authentication of end user. This online service can be integrated with various service delivery applications via an open API.

NIC e-Sign Division carries out the operations and management of integrated ASP gateway for on-boarding NIC applications on to various ESPs (e-Sign Service Providers).

B. Eligibility to Avail Service

The e-sign service is offered to any division in NIC. All applications hosted at NDC, Shastri Park

C. How to register for the service

A single window platform is available for seamless registration of all NIC services, refer **Annexure 1** for more details on online forms.

D. Additional Information

The Application Service Provider (ASP) enables to eSign the application and with the help of Test URL, test the eSign operations through the ASP Gateway. Once successfully tested, the applications which are to be on-boarded on the ASP Gateway have to get all the security audits completed. It is suggested that eSign should not be used for financial transactions.

The application owner can then approach eSign division for on-board the application on the production system. A set of declarations/undertakings are to be signed & stamped by the application authorized person. On receipt of these documents with the copy of valid audit certificate, the public IP of the application server will be white listed. With this the application is successfully on-boarded and ready to use the eSign facility.

E. Complaint Registration

A user friendly service desk portal is available to register complaints related to all services. Refer Annexure 2 for more details.

9. Firewall Access Rule Processing System (FARPS)

A. About

Firewall is a network security system that protects (a network or system) from unauthorized access. It uses rules to control incoming and outgoing network traffic, thus, acting as a barrier between a trusted network and un-trusted network. NIC has deployed high-end firewalls in all of its state of art data centres across India.

B. Eligibility to Avail Service

- The FARPS service is available to all NIC Employees by default and to other Government Officials on the recommendation of concerning HoD / HoG / SIO.
- Users from other departments who avail NICNET facility can use this service through their NIC coordinator.

C. How to avail/on-board the service

- A single window platform is available for seamless registration of all NIC services, refer **Annexure 1** for more details on online forms.
- The approval of FARPS request is done after verifying various security parameters and in compliance with the security policy of NIC. Some of the major pre-requisites for approval are:
  - The Server should be installed with NIC authorised Antivirus software and updated with latest signatures.
  - The Vulnerability Assessment of the server should be completed with a score more than 80and VA report should not be more than 3 months old.
  - The Website/Application involved should have cleared the Application Security audit.

- FARPS has a Notification feature that sends email/SMS to the users on the status of approval and implementation of the FARPS request. Reminder notifications are also sent for the time based rules that are going to expire within a week.

D. Complaint Registration

A user friendly service desk portal is available to register complaints related to all services. Refer Annexure 2 for more details.

10. Gov.in Registration

A. About

The use of GOV.IN domain is for the organizations of Indian Government at various levels right from

- Central Government,
- State/UT Government, and
- District & Sub-District Administration.

B. Eligibility to Avail Service

The eligibility to avail this service is as follows:

- Apex Offices (such as Offices of the Hon'ble President of India, Hon'ble Prime Minister of India) ,
- Ministries of the Government of India Departments; Attached offices Directorates of such Ministries and Departments
- The Ministries of Governments of States which constitute the Union of India Departments; Attached offices/Statutory bodies / Directorates of such Ministries and Departments.
- Local self-Governments and Attached offices of the Local self-Government as defined in under Part IX of the Constitution of India.
- Projects/Schemes/Events/Committees of Ministries
- Departments fully funded by Govt. of India/Governments of States which constitute the Union of India/Local self-Governments (as provided under 3.1(IV) & 3.1(V))
- Law enforcement agencies:
  - Supreme Court of India as established by Part V, Chapter IV of Constitution of India
  - High Courts for the states established under Article 214 of the Constitution of India.
  - Subordinate Courts including but not limited -to all district courts

established by State Governments in India.

- All other bodies created by law, by the assent of Government of India or by the Governments of States of Union of India to perform any other judicial/quasi-judicial functions such as LokAdalats, Tribunals etc.
- All the other Legislative bodies and attached institutions of the Government of India.

· Commissions/Councils created by or under the Constitution of India, statute/executive order of the Government of India or by the executive order of the Governments of states which constitute Union of India.

· Autonomous Societies/Bodies of the Government of India and Governments of States which constitute Union of India. Projects/Schemes/Events/Committees of Ministries/Departments partially funded by Government of India/ Government of States which constitute Union of India.

C. How to register for the service

A single window platform is available for seamless registration of all NIC services, refer **Annexure 1** for more details on online forms.

For more details on service refer to link

https://registry.gov.in/domain_process.html

D. Guidelines

· For Sign-Up to Registry site, email address under @gov.on or @nic.in is compulsory.

· Email under gov.in or nic.in is also essential for entering organizational as well as administrative contacts.

· The organizational and administrative contact should be of two separate persons belonging to the government organization seeking the domain name.

- The signing authority of the forwarding letter should be nodal officer for .GOV.IN or should be the official with designation mentioned online. No equivalent designation is acceptable.
- As per Home Ministry OM issued vide No. 14/4/2001-T dated 17 July 2007, .GOV.IN domain could be hosted on server located in India only.

E. Complaint Registration

A user friendly service desk portal is available to register complaints related to all services. Refer Annexure 2 for more details.

11. SMS Gateway

A. About

In today's e-Governance framework, email and SMS remain the primary means of communication and medium for citizen connect. NIC SMS Gateway allows e-gov applications to integrate with the SMS gateway to send out messages both over data and voice to their user base for maximum impact of an initiative.

Under NIC SMS platform, there is bouquet of services offered to all departments/ministry across Government of India, both at the centre/states and districts. Services include Push and Pull SMS, Short code like 1922 for Mann Ki Baat, 15544 for Mid Day Meal etc. Long code, OBD (Out Bound Dial), Missed Call etc. Gateway has the capability of processing high volume of SMS and OBD/miscall in a day. Milestones includes 14 crores SMS in one day. This platform is integrated with e-Sampark for leveraging the 96.20 crore validated mobile number user base.

Over 1200 applications that includes all major initiatives of the Government are integrated with the NIC SMS gateway. The Various Services Offered under SMS Gateway:

- ✓ SMS PUSH Service [from application to citizens]
- ✓ SMS PULL Service [from citizen to application]
- ✓ OBD [Out Bound Dialling]
- ✓ Missed Call [from citizen to application]
- ✓ Short Code Integration
- ✓ Virtual Mobile Number (long code)
- ✓ OTP SMS Service [high priority SMS]
- ✓ API Based SMS Service
- ✓ SMPP Based SMS Service
- ✓ Web-based SMS Service

- ✓ SMS Analytics

B. Eligibility to Avail Service

This service is offered to all ministries, government departments, PSUs, autonomous bodies, municipal cooperation, govt. societies, educational institutions etc. This service is on paid basis through NICSI as per empanelled rate contract.

C. How to register for the services

A single window platform is available for seamless registration of all NIC services, refer **Annexure 1** for more details on online forms.

D. Guidelines

- Refer https://msgapp.emailgov.in/docs/ for SMS Policy
- Detailed API Integration:
  https://msgapp.emailgov.in/docs/forms/NIC _ API _ Guide.pdf
- Detailed NIC SMS service Integration Document:
  https://msgapp.emailgov.in/docs/forms/Manual_SMS_Gateway.pdf
- IC Service Unicode table:
  https://msgapp.emailgov.in/docs/forms/unicode_table.pdf
- NIC SMS Gateway Integration Guidelines
  https://msgapp.emailgov.in/OnlineForms/NIC-SMS-Gateway-Integration-Guide.jsp

E. Complaint Registration

A user friendly service desk portal is available to register complaints related to service. Refer Annexure 2 for more details.

12. Virtual Private Network

A. About

VPN stands for Virtual Private Network which is a mechanism of extending a private network over public network to allow access of internal resources. It uses a suite of security protocols to achieve IP-in-IP encapsulation which forms a virtual tunnel to transport communication for internal resources over public network hidden from unauthorized users.

NIC provides VPN for securely accessing the services hosted within NIC Data Centres. It is also commonly used for strong access control mechanism as it uses Two Factor Authentication (2FA) for users by means of a Digital Signing Certificates (DSC) and a password. So critical services which need controlled access and strong user authentication widely use NIC VPN.

VPN is provided for the following requirements,

a) Administrative access to resources hosted in NIC Data Centres across the country. Administrative access means SSH, Telnet, FTP, RDP, Database or any other service which can be used change the system which can affect the service at large.
b) Administrative access to NIC Cloud resources for administration.
c) Extending access to internal resources to users stationed outside NICNET.
d) Restricting access to resources to a limited set of users.
e) Communication between servers hosted in NIC Data Centres and Data Centres outside NICNET.

The following types of VPN are offered,

(i) **Remote-access (RA) VPN**– is used for accessing services by users with the help of DSC and VPN client on individual client machines. This type of VPN mandatorily requires a human being at the client machine to connect VPN manually, access the resources and disconnect. The first four requirements mentioned above are

serviced using this type of VPN.

(ii) **Site-to-site VPN** – is used in case of server to server interaction without human intervention. Here a tunnel is created between two network devices sitting at the gateway of the two data centres hosting the two servers and they create a VPN tunnel for the servers to communicate. The last requirement mentioned above is catered to using this type of VPN.

B. Eligibility to Avail Service

VPN accounts can be provided to any user (government as well as non-government employee) of NIC services who has any of the requirements mentioned above. However, the concept of trust chain is the central theme. Trust chain consists of the user (applying for VPN), her/his Head of Department (HOD) / Reporting Officer (RO), NIC Coordinator for the respective department and the VPN team. The trust/responsibility of actions flows in this chain. It means that the VPN team trusts the NIC Coordinator only and is not concerned about the user or her/his HOD/RO. Conversely, the NIC Coordinator trusts the HOD/RO of the respective department and is not concerned about the user. The actions of the user is the responsibility of her/his HOD/RO.

C. How to register for the service:

A single window platform is available for seamless registration of all NIC services, refer **Annexure 1** for more details on online forms.

i. **New Individual Accounts**– After filling the form a PDF file is generated. Users need to print this form and sign it. Get it signed and stamped by their HOD/RO and forward it to NIC Coordinator. The NIC Coordinator has to sign & stamp the form at the designated place, scan it and mail it to the email address **vpnsupport@nic.in** from their official email addresses only.

ii. **New Bulk Accounts**– are created for a group who need same access permissions for accessing same resources. They can be obtained by

filling one online application form by the project leader/coordinator and attaching the list of other users in the format available at point **F** below. The project coordinator's form along with the list of other users have to be signed and stamped by the HOD/RO and then by NIC Coordinator and forwarded to **vpnsupport@nic.in** as mentioned above. Please remember to attach the list in excel format along with project coordinator form.

iii. **New Cloud Accounts**– are provided along with the cloud account and no separate form has to be filled separately for it.

iv. **Renewal** – is a just term used to refer to an existing user. Technically, the DSC issued for VPN are time-bound self-destructible entities valid for two years only which cannot be extended. So the users need to follow the same procedure as done for new accounts.

v. **Add/Modify Permissions**– can be made using online add/modify form or offline CR Form, both available at eforms.

vi. **Modify User Details**– can be done by creating a NIC Service Desk ticket from the registered email address and mobile number.

vii. **Surrender/Loss**– can be reported by creating a NIC Service Desk ticket from the registered email address and mobile number.

viii. **Update NIC Coordinators**– can be done by filling the Coordinator Authorization Form available at eforms

ix. **Other Requirements**– including site-to-site VPN should be sent to HOG (Operations and Routing) with requirement and other details.

x. **Troubleshooting** – Any issue can be reported through NIC Service Desk only. There are no dial-in numbers for VPN support. The users need to create a ticket at NIC Service Desk and the VPN support will call the users on the contact number provided in the ticket. All software, procedures and manuals are available at the website eforms.

D. Complaint Registration

A user friendly service desk portal is available to register complaints related to service. Refer Annexure 2 for more details.

13. Video Conferencing

A. About

NIC provides Video Conferencing which includes Studio based, Cloud based (Web based) and Event based Video conferencing services

Key features and milestones of NIC's Videoconferencing services are:

- NIC is offering state of art Full High Definition (HD) Videoconferencing services over NICNET since 1995
- NIC has 1600+ Videoconferencing studios over NICNET spread across the country at State Capitals, Districts, Union Territories, and Ministries etc.
- An average of 28,000 multi-site Videoconferences with more than 600,000 site-hours of Videoconferencing sessions are being held annually.
- NIC's Cloud based (WebVC) Desktop Videoconferencing services are being used by more than 20,000 users from Central & State Government, NKN, e-Court, DFS etc. with more than 3, 00,000 hours of VC usage annually.

B. Eligibility to Avail Service

This service is offered to Officials of Central and State Government Ministries/Departments.

C. How to register for the service

A single window platform is available for seamless registration of this service, refer **Annexure 1** for more details on online forms.

D. Complaint Registration

A user friendly service desk portal is available to register complaints related to service. Refer Annexure 2 for more details

14. Vulnerability Assessment

A. About

Vulnerability Assessment Service aims at identifyingweaknesses and vulnerabilities (flaw in a system that can leave it open to attack) in a systems design, implementation, or operation and management, which couldbe exploited to violate the systems or organisations security policy. NIC has inplace Vulnerability Management System which performs VA (both OS and DB) on theservers of NIC deployed in its data centres across the country.

B. Eligibility to Avail Service

The VA service is available to all NIC employees serving as System/Database Administrator. Users from other departments who have their servers deployed in NIC data centres can also avail this service through their NIC coordinator. Additionally, VA service is also used by the VA Administrators for periodic VA of the servers / DBs.

C. How to register for the service

A single window platform is available for seamless registration of all NIC services, refer **Annexure 1** for more details on online forms.

Using this application, user can avail the following services.

- Request for VA of OS/DB.
- View the Status of VA request.
- View the List of Pending/Completed Request.
- Download the VA Report.

D. Guidelines

As per Cyber Security Policy of NIC (**https://security.nic.in**, accessible over **NICNET**), the following things need to be complied.

- VA should be done for the servers before being deployed in NIC Data centre.

- VA of the servers needs to be repeatedly performed every three months.
- System administrator should ensure the patching of all the vulnerabilities highlighted in the VA report and request for a rescan.
- The rescan report should not have any vulnerabilities left, be it LOW/MEDIUM/HIGH/CRITICAL.
- Clearing of VA is mandatory for the approval of Firewall requests.

VA application has a Notification feature that sends email notification to the VA admin to scan the server and to the users/requester to download the scan report from the site once scanning has been completed.

E. Complaint Registration

A user friendly service desk portal is available to register complaints related to service. Refer Annexure 2 for more details.

15. Web Application Firewall (WAF)

A. About

To overcome the web application threat attacks, WAF is positioned for strengthening and enhancing the application level security of NIC. It will block an ever expanding list of sophisticated web-based intrusions and attacks that target hosted applications.

The key security features to be provided by the WAF solution are as follows:

- Brute Force Attack prevention and Application denial of service (DoS) protection – Slow Client Attack, DDoS Prevention using CAPTCHA, IP Reputation Filter
- Scanning of all inbound web traffic to block attacks, and inspection of HTTP responses from the configured back-end servers for Data Loss Prevention (DLP).
- Protection against common, high-visibility attacks – SQL injection, Cross Site Scripting, Command injection, CSRF, XML attacks, Malicious File Execution and zero-day attack protection.
- Protection against attacks based on session state – Session Hijacking, Cookie tampering, Click jacking
- Data Theft Protection – Deep inspect of all server responses to prevent leakage of sensitive information using provided default patterns (credit card data etc.) or User Defined Patterns (custom Patterns)
- Website Cloaking – Strips identifying banners of web server software and version numbers and provides customizable HTTP error handling to defeat server fingerprinting attacks (Suppressing error codes and filtering headers)
- Logging, Reporting and Monitoring – Inbuilt reporting module, Web Firewall Logs, Access Logs, Audit Logs, Configuring syslog.
- Restricts the access of critical part of application like CMS for defined Trusted IP(s).
- Support for handling SSL/TLS based applications.

B. Eligibility to Avail Service

Application Firewalls are deployed in National Data Centre Shastri Park and Hyderabad. Hence, websites / applications hosted in these two data centres only can avail the services of Web Application Firewall.

C. How to register for the service

A single window platform is available for seamless registration of all NIC services, refer **Annexure 1** for more details on online forms.

A filled-in, signed and approved form is to be sent to Application Security Group (ASG) at e-mail id: **appsemon10@nic.in**

D. Guidelines

Following are the steps to host the website with protection through WAF:

- ASG would open ports from WAF to Application Server/Load Balancer (LB)
- ASG would configure the Website on WAF and provide the Virtual IP for local client testing to user
- User has to browse the application thoroughly and check for any false positives
- For any false positives, ASG would create appropriate rule-sets in the configuration on WAF
- After confirmation from user, ASG would make live the application hosted behind WAF by changing the NAT of DNS Public IP with WAF Virtual IP
- Further, the web application would be regularly monitored 24x7 through Web Application Firewall for expected protection from application level attacks

E. Complaint Registration

A user friendly service desk portal is available to register complaints related to service. Refer Annexure 2 for more details.

16. Webcast

A. About

With the advent of high end streaming media technology, the concept of doing live/on-demand webcast has gained popularity like never before. Webcasting an event allows you to extend the reach of your event to all corners of the world, with no limitations of physical or geographical boundaries. At NIC, we ensure that your events get an optimum webcast with flawless production quality. NIC's webcast service offers a turnkey solution for an event, bringing onsite production, hosting, and streaming to millions of online viewers. Webcast service is offered under following category:

- **Live Webcast**: Transmission of live or pre-recorded audio or video to personal computers that are connected to the Internet. A user who clicks a link to a live clip joins the live event in progress. Because the event is happening in real time, fast-forward, rewind, and pause capabilities are not available. Live Webcasts are most suitable for high demand live presentations to large geographically dispersed audiences. Participants can attend these virtual presentations from their desktop by visiting a web site. It makes interaction between instructor and learners occurs in real-time. Participants can use a chat window to type in questions to the presenter during the session. Webcasts simulate the look and feel of a live event and can even be recorded for later viewing for those who missed the original web cast. This method is also less expensive than satellite broadcasting.
- **On-Demand Webcast:** Pre-recorded clips are delivered, or streamed, to users upon request. A user who clicks a link to an on-demand clip watches the clip from the beginning. The user can fast-forward, rewind, or pause the clip. Therefore on demand streams can be created from archived live events or recorded clips.

B. Eligibility to Avail Service

This service is offered to Central and State Government institutions only.

C. How to register for the service

A single window platform is available for seamless registration of all NIC services, refer **Annexure 1** for more details on online forms.

D. Complaint Registration

A user friendly service desk portal is available to register complaints related to the service. Refer Annexure 2 for more details.

E. Additional Information

This service is a value added paid service.

17. Wi-Fi

A. About

NIC has deployed centrally managed Wi-Fi service, this service is offered free of cost to all government offices wherever NICNET is present. Latest Wi-Fi protocols and security policies are implemented to provide secure and reliable Wi-Fi access across location. The service provide seamless roaming which allows user to use the Wi-Fi service not only at their base location but also at other NIC locations with the same user profile.

The key feature of Wi-Fi services are

- ✓ Centralize network operations.
- ✓ High availability of wireless for both HQ and State.
- ✓ Guest Access to wireless network.
- ✓ Integrate with existing LDAP server for authentication Wireless.
- ✓ Connectivity for the MPLS VPN users.
- ✓ Seamless Mobility for WLAN Services.
- ✓ Dynamic RF Management.
- ✓ Centralized Management.
- ✓ Planning and troubleshooting.
- ✓ Security Management (IDS/IPS).
- ✓ Location Tracking.

B. Eligibility to Avail Service

This service is offered to users having **@gov.in / @nic.in** email ID provided by NIC.

C. How to register for the service

A single window platform is available for seamless registration of all NIC services, refer **Annexure 1** for more details on online forms.

D. Complaint Registration

A user friendly service desk portal is available to register complaints related to the service. Refer Annexure 2 for more details.

Annexure 1

(Single Window for Registration of NIC core Services – eForms)

https://eforms.nic.in is the single window platform for seamless registration of all NIC services. The Objective of this portal is to provide an easy registration window for all users who want to avail NIC services. This portal implements all the security measures and provides e-Signing facility to sign the documents online.

In day to day activities, we use conventional paper forms (hard copies) for making a request for registration and which is duly signed and stamped by user, Approving Authority and NIC coordinator. Keeping in mind the numerous hurdles a user might face while filling up the forms manually, this portal has been developed to provide effectiveness, efficiency and tracking in the registration process

Online Forms takes care all these challenges and provides an effective solution by implementing approval workflows. Documents are digitally signed and routed to the respective NIC coordinators. User can track their request anytime anywhere and are free to cancel/edit the request if they find any error even after submitting the form. This tracking facility is available to all the stakeholders in the process i.e. users, Approving Authority, NIC Coordinator and Administrators. In addition to online web tracking facility, all the stakeholders are also notified through e-mail and SMS about the requests routed to them for an early action and response.

If the users are not satisfied with any aspect of **eforms**, they can send their feedbacks to **eforms@nic.in**. It will be taken constructively and help NIC improve the portal.

Annexure 2

(Service Desk)

NIC Service Desk is a single-window platform for resolving issues related to various services offered by NIC.

Anyone availing the NIC services can register their complaints regarding any service offered by NIC by going to the website **https://eforms.nic.in** or call the toll free number **1800-111-555**. If going through the web portal, Users need to enter their contact and location details correctly after verifying their email address or mobile number through OTP for quick resolution and response.

Any user of NIC services including the government, statutory bodies or general public can raise a trouble ticket for the issues faced by them. The users can raise trouble tickets for any issue related to any service from a single website or by dialling a single toll free number without scrambling for the correct contact. The service desk will ensure that the trouble ticket is routed to the correct team in the shortest possible time. The main objectives of NIC Service Desk are:

- ✓ Single point of contact for users for all NIC services
- ✓ Fastest possible routing of issues to the concerned
- ✓ Transparency and accountability in handling of issues
- ✓ Single repository for issues raised and serviced
- ✓ Timely resolution with provision for escalations
- ✓ Detailed response to users' issues with a mechanism for feedback
- ✓ Communication channel between NIC and its users
- ✓ Improved experience with NIC services

Users can also view of the status of their tickets on the same website at the Previous Ticket tab. Ticket status can be checked, priority increased and

escalation for the ticket can be done through the toll free number after quoting the ticket number.

Any attachment to the ticket can be sent through the email by replying to the initial email sent at the time of ticket registration. If the issue is not resolved, please reply to the email response received from the service teams and the ticket will automatically re-open.

The service teams will call the users within a stipulated time when a ticket is raised.

If the users are not satisfied with any aspect of NIC Service Desk, they can send their feedbacks to **nsd-admn@nic.in.** It will be taken constructively and help NIC improve the service.

Editorial Board

NATIONAL INFORMATICS CENTRE
A Block, CGO Complex
Lodhi Road, New Delhi 110003
eMail: handbook@nic.in