Service Level Agreement

1.Service Objective:

1.1 The objective of the implementing agency is to provide a centralized Messaging service to all employees working under the different arms of the Government, both at the Central and State level that:

- Is efficient
- Is scalable and reliable
- Satisfies the security requirements of the Government
- Meets the needs of its users

2.SLA Objective:

2.1 The purpose of this Service Level Agreement is to clearly define the levels of service which shall be provided by the implementing agency to its users.

3.Scope of Service Level Agreement:

3.1 This document describes the standard level of service that would be rendered by the implementing agency within the framework of Security, including performance criteria, availability of services, action to be taken in cases of a service failure and response and repair times.

3.2 The implementing agency reserves the right to change, update, amend or modify this SLA at any time. Such changes will be intimated to the users.

4.Additional Definitions

4.1 For the purpose of this agreement, the following additional definitions are required:

4.1.1 False positive - means a wrong classification of a legitimate email message as spam or Malware by scanning techniques and, as a result, interfering with its delivery.

4.1.2 Known Malware - means malware which is detectable with existing anti-virus software signatures known to the anti-virus software used as part of the Service.

4.1.3 Repair time - means the time within Office hours measured by the implementing agency between the implementing agency receiving a notification of a failure by the user and recovery of the Service by the implementing agency.

4.1.4 Scheduled maintenance - means maintenance work performed by the implementing agency to its own network, data center, servers and resources. Implementing agency will notify the users about the maintenance and the expected time for service restoration will be notified on the website.

4.1.5 Service Availability - means the amount of time expressed as a percentage during which the Service is available for the user over a defined period.

4.1.6 Service failure - means an interruption of the delivery of Services and Deliverables excluding Scheduled maintenance.

5.Service uptime Levels:

5.1 The Messaging Services shall generally perform to the levels as set forth below:

S.No	Service Levels	uptime	Remarks
1.	Service Availability (per year)	99.9 %	It may also be noted that in a single instance, in case of the primary site is down for a period beyond 60 minutes, the process of Disaster Recovery will be initiated and service will be restored from the DR site. The service will be restored within 45 minutes from DR initiation.
2.	Mail delivery	100 %	This does not include mails with infected attachments/ message size exceed/ disallowed attachment type/blacklist sender address/ blacklist IP address/Mail from an open relay/ any other violation of the messaging usage policy
3.	Time within which mail will be delivered within the same domain	Within 5 minutes	Implementing agency will make best efforts to ensure instant delivery. However, it does not include instances beyond the control of implementing agency that include large queue size due to large attachment , DOS attack etc which results in delay in delivery.

4.	Time within which mail will be delivered to outside servers	Within 5 minutes mail will be sent outside NICNET	Implementing agency will ensure that the mail is sent to the destination server within 5 minutes however, Implementing agency will not be responsible for mail delivery to domains and recipients outside NICNET under the conditions mentioned in Annexure E(1) enclosed with this SLA.
5.	Malware Detection	100%	The gateway appliance has been configured with two well known AV scanners. As per security policy, each desktop also has an AV scanner. Hence each mail/attachment is scanned with atleast 3 scanners. Implementing agency will ensure malware detection of known malware, for which signatures are available for the Anti-Virus and Spam scanners configured in the Messaging System. This does not cover zero day/targeted attacks.
6.	Repair Time	According to the Operational SLA defined below	
7.	False Positive	0 %	No mail is dropped as a result of a false positive. Any mail detected as a false positive is

			flagged as "Spam" and delivered to the users "Probably Spam" folder. User needs to check the folder once a day

6.Operational SLA

6.1 Operational SLA for Services would be defined in the following categories:

Severity level*: The severity level of a service call is defined by the extent of impact the problem has on the overall performance of the Solution*

S1- Very high severity: Complete failure of critical systems, services, applications or Network All user base is impacted with the downtime.

S2- High Severity: Application is not down but there is a serious problem affecting productivity of important/multiple users

S3- Medium Severity: Application is not down but there is an issue affecting a small number of users

S4- Low Severity: Functionality enhancement and/or support for modifications or maintenance of source code, training documentation or user documentation.

6.2 The list of typical events with the Severity level is given below. However, the event can be a single event or greater than all events combined together, for a single user/ domain or combination of all together and collectively known as the "total solution".

6.3 In case of a total service shutdown due to any reason like power/flood/network collapse the service would be provided from the Disaster Recovery site. For details refer to Business continuity mentioned in Annexure "A". The problems mentioned below are only the ones that are caused within the system.

	Problem Description	Severity Level	Problem code	Repair Time (in hrs)
1	Mail not coming	S1	Err01	0.30
2	Outgoing mails are not delivered by gateway	S1	Err 02	0.30
3	Taking time to open an email/attachment	S3	Err 03	0.15
4	Taking lot of time to authenticate	S2	Err04	0.15
5	General Authentication failure	S1	Err05	0.30
6	Authentication fails with OTP and virtual keyboard	S2	Err06	0.30
7	Authorized users are not able to send mail	S1	Err07	0.30
	Delay in incoming mail	S3		

	Problem Description	Severity Level	Problem code	Repair Time (in hrs)
8			Err08	0.30
9	mails missing/not delivered	S3	Err09	0.15
10	Recipient domain not receiving mails	S3	Err10	0.15
11	Security breach & RCA (Root Cause Analysis)	S1	Err11	24 hrs
12	OS not coming up	S1	Err12	Service will run from DR
13	Valid mails are getting queued and could not be delivered	S3	Err13	0.30
14	MTA service not working	S1	Err14	0.15
15	Calendar Service not working	S2	Err15	0.15
16	Address book service not working	S2	Err16	0.15
17	IM service not working	S3	Err17	0.15
18	POP(S) service not working	S1	Err18	0.15

	Problem Description	Severity Level	Problem code	Repair Time (in hrs)
19	IMAP(S) service not working	S1	Err19	0.15
20	webmail service not working	S1	Err20	0.15
21	Message store service not working	S1	Err21	0.30
22	S/MIME service not working	S3	Err22	0.15
23	Application upgrade not done in time	S3	Err23	12 hrs
24	OS upgrade not done in time	S3	Err24	12 hrs
25	Delay in Fixing of bugs and vulnerabilities	S1	Err25	12 hrs
26	Delay in applying patches (that causes issues in the setup)	S1	Err26	12 hrs
27	Service malfunctions after OS/Application upgrade	S1	Err27	Service will run from DR

7.Reporting and Complaint Registration:

7.1 The implementing agency operates a 24x7 Support cell for complaint registration and for providing online support. Subsequent to complaint registration, a ticket is issued and the approximate time for problem resolution is given to the person registering the complaint.

7.2 Complaint can also be registered by sending a mail to support@gov.in**. A toll free** number for contacting the Support cell will be published on the Messaging services website.

8.Escalation Matrix:

8.1 The escalation matrix for resolving a issues is as follows:

8.1.1 Call is registered with 24x7 iNOC support helpdesk and a ticket is assigned (L0)

8.1.2 Subsequent to call registration the problem is handled by L0/L1

8.1.3 If the issue is not resolved within the time frames indicated above L2 will look into the issue

8.1.4 In case the issue becomes critical, then it will be escalated to L3.

- Implementing agency will not be responsible if a mail delivery to a domain and a recipient outside NICNET fails under the conditions mentioned below. It may be noted that the list of codes shown below are based on the Extended SMTP (ESMTP) standards, where X can be 4 or 5, depending on the error type (Persistent Transient or Permanent):

- X.1.0 Other address status
- X.1.1 Bad destination mailbox address
- X.2.0 Bad destination system address
- X.1.3 Bad destination mailbox address syntax
- X.1.4 Destination mailbox address ambiguous
- X.1.5 Destination mailbox address valid
- X.1.6 Mailbox has moved
- X.1.7 Bad sender's mailbox address syntax
- X.1.8 Bad sender's system address
- X.2.0 Other or undefined mailbox status
- X.2.1 Mailbox disabled, not accepting messages
- X.2.2 Mailbox full
- X.2.3 Message length exceeds administrative limit.
- X.2.4 Mailing list expansion problem
- X.3.0 Other or undefined mail system status
- X.3.1 Mail system full
- X.3.2 System not accepting network messages
- X.3.3 System not capable of selected features
- X.3.4 Message too big for system
- X.4.0 Other or undefined network or routing status
- X.4.1 No answer from host
- X.4.2 Bad connection
- X.4.3 Routing server failure
- X.4.4 Unable to route

- X.4.5 Network congestion
- X.4.6 Routing loop detected
- X.4.7 Delivery time expired
- X.5.0 Other or undefined protocol status
- X.5.1 Invalid command
- X.5.2 Syntax error
- X.5.3 Too many recipients
- X.5.4 Invalid command arguments
- X.5.5 Wrong protocol version
- X.6.0 Other or undefined media error
- X.6.1 Media not supported
- X.6.2 Conversion required and prohibited
- X.6.3 Conversion required but not supported
- X.6.4 Conversion with loss performed
- X.6.5 Conversion failed
- X.7.0 Other or undefined security status
- X.7.1 Delivery not authorized, message refused
- X.7.2 Mailing list expansion prohibited
- X.7.3 Security conversion required but not possible
- X.7.4 Security features not supported
- X.7.5 Cryptographic failure
- X.7.6 Cryptographic algorithm not supported
- X.7.7 Message integrity failure