Sandes Gateway Service Usage Guidelines

1. Sandes gateway integration must be implemented only using the gateway client service.

2. Always ensure that the latest version of gateway client service is deployed on your production. The deployed version of Sandes gateway client version in your servers and the latest available version are provided in the daily statistics email.

3. The maximum length of a message request is limited to 5 KB and a request crossing this limit would be rejected by the gateway.

4. The daily, weekly and monthly messaging statistics for the app account are shared to the technical contacts by email on a daily basis.

5. The dispatch, delivery and read statistics for a message request would be made available for up to 10 days from the message request date. This status can be queried using the message status API provided by the gateway client service. The message dispatch count between any two given dates can be queried using the message stats API provided by the gateway client service.

6. The encrypted files shared through Sandes gateway would be retained for a period of 3 months.

7. The messages/files sent from gateway client service Ver. 1.6 or above are end-to-end encrypted by default, to ensure security and privacy of messages.

8. It is not advisable to send sensitive messages without E2EE. Sensitive messages are those containing personal identifiers, security tokens, OTPs, credentials, internal application logs, audit trails or any information that is restricted from public access as per organization policies.

9. End-to-end encryption can be disabled explicitly for non-sensitive messaging / message broadcasts to optimize for dispatch speed.

10. Sandes gateway client service and credentials must be removed from development machines after completing integration.

11. The IP whitelisted for your app account must be periodically reviewed and request to remove unused IP addresses must be sent to sandes-support@nic.in

12. The *high-volatile* priority setting must be used only for sending OTP messages. Any other message requiring high priority QoS must be submitted only using *high* priority setting.

13. The rate limiting plan must be based on the peak concurrent messaging rate required by your application.

14. The periodic/scheduled broadcast jobs must adhere to the configured rate limiting plan to avoid queuing of requests. This can be achieved by adding suitable delay between message requests during a batch messaging / broadcast.

15. Wherever Sandes gateway is used as a primary channel for communication, it is advisable to have an alternate channel as a backup to ensure your service availability. For example, if OTP delivery is integrated using Sandes gateway, the resend OTP request may be configured to send Sandes OTP along with SMS / email OTP.

16. Always mention your client ID in all communications with Sandes support.

17. Do not send your client secret or HMAC key in your communication with Sandes support.

18. Ensure that access to both Sandes Gateway Production and Sandes Gateway DR are allowed from your production server.