NFS Business Resiliency Statement

The objective of this Business Resiliency Statement is to place the commitment of National Payments Corporation of India (NPCI) to the stakeholders (Members Banks and Customers at large) to operate the National Financial Switch on a 24x7 basis with near zero downtime and zero tolerance to data loss. The commitment is established with the following operational framework:

1. At the Data Centre in Mumbai, critical components like Server, Storage, Network, Power supply have been provided with adequate redundancy thus keeping fall back arrangements readily available at times of failure of any one or more of these components. Mumbai Data Centre functions as the Primary Data Centre for ATM & RuPay and DR Data Centre for IMPS & AEPS.

2. A back-up server is available at the Primary Data Centre as a high-availability system and can take over the services of the Primary Server within a short duration of about 15 minutes. Data replication between Primary and high availability system takes place on a real time basis. High-availability system is of identical configuration to be able to process similar transaction volumes.

3. The redundancy provided at the primary Data Centre is regularly tested to ensure that they are functional at any point of time.

4. The offsite Disaster Recovery (DR) Data Centre located in Chennai, is in a different seismic zone. A high availability server is available at the Chennai Data Centre too. Chennai Data Centre functions as the Primary Data Centre for IMPS & AEPS and DR Data Centre for ATM & RuPay. High-availability system is of identical configuration to be able to process similar transaction volumes.

5. The Primary and the DR Data Centre are connected with each other by means of four lease lines, two with a bandwidth of 200 Mbps and the other two with a bandwidth of 100 Mbps. Data replication between Primary and Disaster Recovery Servers takes place on a real time basis to ensure compliance to RPO / RTO.

6. The Offsite DR Data Centre can be brought up anytime to provide business continuity within 45 minutes, without loss of any transactional data, in case of non-availability of the Production & High Availability server at the Primary Data Centre.

7. The Information systems at both the Primary and DR Data Centres, periodically undergo Information System Security Audit, by experienced Information System auditing firms. Any change in network architecture is reviewed & approved by Information Security team and is audited by NPCI Internal audit team & experienced External audit firm at regular intervals.

8. All our member banks connect to NFS using NPCI’s data communication private network known as NPCINET. Our Migration from Primary to DR and back from DR to Primary Data Centre is transparent to the member Banks.

9. There are operation support teams available at both the Primary and DR sites so that recovery operations are resumed immediately when there is a need for bringing up the DR site.

10. There are technical support teams available at both Primary and DR sites so that technical support is available immediately when there is a need for activating the DR site.

11. Disaster recovery drills are performed on a quarterly basis to test the RTO and RPO as well as capability of the team and systems to handle production loads. Once a year a surprise failover drill is conducted to check readiness of all support teams.

12. To ensure functionality of these systems, NPCI has been certified for ISO 22301 for these locations.