Recommendations

on Business Continuity of AZIPS/RTGS participants in emergency cases

1. An emergency response plan should cover various possible cases, including disasters, equipment failure, terrorism, external penetration, and downtimes due to communication lines failure and provide for recovery of activities of participants in the AZIPS within 2 (two) hours per case.

2. Participants should ensure launch of critical infrastructure equipment, system configuration (updates and changes to hardware and software), alternate communication lines, UPS and fire extinguishers in a back-up center, similar to those in use in the main center and maintain their periodic review and update.

3. Real time data replication should be used with the backup center.

4. The backup center should be ready to conduct operations in a real time mode, and staff should be provided with necessary conditions for long term performance there.

5. To validate the level of preparation for emergency cases participants should conduct real time operations via the backup center at least 4 times a year.

6. To conduct data sharing in emergency cases participants should designate and accordingly instruct relevant employees (main persons and substitutes).

7. Participants should maintain a register on the cases that led to break of activities and include the details, time, elimination period and works done with respect to particular case there.