APPENDIX 1: SUMMARY OF AMENDMENTS

Previous Provision	New Provision/Amendments	Explanatory Notes
This is a new provision.	**Section 4.1.3 Cyber Security Risk Management Measures** A Participant shall at a minimum: • **Cyber-Risk Management Framework** Put in place a cyber-risk management framework to mitigate against cyber-attacks on the ZIPSS. The cyber-risk management framework shall prescribe measures to be taken by a Participant to fully recover its operations where a cyber-breach affects its operations. • **Restricted Physical Access** Physical access to ZIPSS workstations including at the fall back sites shall be restricted and strictly controlled from being accessed by unauthorized persons. • **Segregation of Duties** Participants shall ensure segregation of duties by creating profiles that separate business functions and duties. • **Token Management** Each User shall ensure that their e-token is kept safely at all times. The e-token default password should be changed when the User logs in for the first time and the new password should not be shared. • **Password Management** Users shall create strong and unique passwords whose complexity shall have a minimum of eight characters, a combination of upper and lowercase letters and either a number or symbol/special character. Users should	Section 4.1.3 has been introduced to the ZIPSS rules on the requirement for all Participants in the ZIPSS to secure ZIPSS interfaces against cyber-attacks.

	ensure that the passwords are changed regularly and that they are never shared with another person. • **Monitoring Tools** Implement monitoring tools/capabilities that are able to identify and prevent system breach. • **Detection of Breach** Where a breach is detected, the tools/capabilities must quickly identify the breach and quarantine the threat to minimise impact, loss or damage. • **Prevent Reoccurrence** Ensure that measures are put in place to prevent reoccurrence of an attempted or successful breach. • **Cyber-Risk Assessment** Undertake regular cyber-risk assessment, and review effectiveness of internal cyber risk controls. • **Cyber Security Awareness** Participants shall undertake cyber-risk awareness among its staff and users of the ZIPSS and any other relevant stakeholders. • **Cyber Security Incident Response Guide** Each participant shall have in place an incident response plan to deal with material cyber security breaches or attempts. A recovery and assurance plan shall ensure system's integrity following the cyber security incident as well as recovery of lost or corrupted data due to the cyber security incident. • **Cyber Communication and Information Sharing Strategy** Each participant shall report major breaches to the BoZ within 24 hours of discovering the breach. The incidents shall be reported through email at zipss@boz.zm.	

	- **Appointment of Participant Security Administrators** Each Participant shall designate among its staff a minimum of two Participant Security Administrators who shall be responsible for communication with BoZ and executing tasks regarding: a) The set-up of Users; b) Amendment of User profiles; c) Removal of Users from the system, and d) The management of e-token and certificate issue and delivery to end-Users. BoZ shall maintain the list of Participant Security Administrators.	
10. Processing Procedure **10.1 General Issuing Conditions** Participants shall comply with the time table in Annex 7 and shall undertake to present the different types of Payment Instructions before the cut-off times stated in this timetable. Participants wishing to apply for an extension of the cut-offs on ZIPSS shall be required to do so no later	10. **Processing Procedure** Participants shall comply with the timetable in Annex 7 and shall undertake to present the different types of Payment Instructions before the cut-off times stated in this timetable. Participants wishing to apply for an extension of the cut-offs on ZIPSS shall be required to fill out the form in Annex 18. The completed application shall be signed by two (2) authorised signatories and shall be sent to zipss@boz.zm no later than 15:30 hours. The conditions under which the Bank shall consider to extend the system include the following: i. System wide challenges on the ZIPSS;	**Section 10 – Processing Procedures** This section has been enhanced to provide conditions under which the Bank shall consider to extend the system cut-off times on the ZIPSS beyond the ZIPSS operating timetables.

than 15:30 hours. Such application shall be done IN WRITING, addressed to the office of the Assistant Director – Payment Systems, indicating the reason for the request to extend. The Bank shall determine the duration of the extension and shall not extend the system by more than 45 minutes from the default cut-off time. The Bank of Zambia reserves the right to reject or deny such application for extension of the cut-off times on ZIPSS. Participants should monitor the messages in the outward ZIPSS Pending Queue and take the necessary action to clear any ZIPSS transactions in the outgoing Pending Queue before the Final Cut-Off. Transactions that do not settled at final cut-off shall	ii. System wide challenges on ZECHL operated payment platforms (EFT, CIC and NFS); iii. Processing of systemically important/critical payments; iv. Challenges impacting the ZIPSS on account of integration with other critical infrastructures; v. To facilitate system maintenance; and vi. Challenges with the ZIPSS infrastructures. Where all or a significant number of Participants fail to access the system via the SWIFT network or VPN. BoZ shall determine the duration of the extension and reserves the right to reject an application for extension. An approved application for extension shall attract a fee as prescribed by the Bank. Participants shall monitor the messages in the outward ZIPSS Pending Queue and take the necessary action to clear any pending transactions before the Final Cut-Off. Transactions that do not settle at final cut-off shall be cancelled and shall attract a charge as detailed in Annex 8 – Pricing.	

be cancelled and attract a charge as detain in Annex 8 – Pricing.		
Section 17 – Audit Rules Each Participant must submit to BOZ a yearly compliance audit certificate, in the form specified in Annex 11, within 60 calendar days of the anniversary of the Participant joining ZIPSS. The yearly compliance audit certificate must be signed by a duly authorised officer of the Participant. Any evidence of that authorisation which is reasonably requested by BOZ must be promptly produced to BOZ following that request.	**Section 17 – Audit Rules** Each Participant shall submit to BOZ a yearly compliance audit certificate for the preceding year by 31st March of every calendar year, in the form specified in Annex 11. The yearly compliance audit certificate must be signed by the Chief Operating Officer and the Compliance Officer.	**Section 17 – Audit Rules** This section has been amended to provide a date of submission for the ZIPSS yearly compliance audit certificates.