




ANCILLARY SERVICE PROVIDERS GENERAL REQUIREMENTS MODULE

 Central Bank of Bahrain Rulebook	Volume 5: Specialised Licensees (Ancillary Service Providers)
MODULE:	GR (General Requirements)
Table of Contents	

	Date Last Changed
GR-A Introduction GR-A.1 Purpose GR-A.2 Module History	04/2016 xx/2023
GR-B Scope of Application GR-B.1 Ancillary Service Provider Licensees	04/2016
GR-C Provision of Financial Services on a Non-discriminatory Basis GR-C.1 Provision of Financial Services on a Non-discriminatory Basis	10/2020
GR-1 Confidentiality GR-1.1 General Requirements	04/2016
GR-2 Books and Records GR-2.1 General Requirements GR-2.2 Transaction Records GR-2.3 Other Records	04/2016 01/2020 04/2016
GR-3 Publication of Documents by the Licensee GR-3.1 General Requirements	04/2016
GR-4 General Requirements for TPAs GR-4.1 Compensation GR-4.2 Code of Conduct GR-4.3 Segregation of Funds GR-4.4 Content of Written Agreement GR-4.5 Prohibition of Collection of Premiums/Contributions	04/2016 04/2016 01/2017 04/2016 04/2016
GR-5 General Requirements for Credit Reference Bureaus GR-5.1 Code of Conduct	04/2016
GR-5A [This Chapter has been deleted in April 2022 and replaced with Module CFP requirements] GR-5A.1 This Section was deleted in April 2022 GR-5A.2 This Section was deleted in April 2022	04/2022 04/2022
GR-5B Security Measures for Payment Service Providers Owning or Operating Cash Dispensing Machines (CDMs) or Kiosks GR-5B.1 Physical Security Measures for Payment Service Providers Owning or Operating Cash Dispensing Machines (CDMs) or Kiosks GR-5B.2 CDM/Kiosk Security Measures: Hardware/ Software	07/2020 04/2019

MODULE:	GR (General Requirements)
Table of Contents	

	Date Last Changed
GR-6 Dividends	
GR-6.1 CBB Non-Objection	10/2017
GR-7 Controllers	
GR-7.1 Key Provisions	04/2019
GR-7.2 Definition of Controller	04/2016
GR-7.3 Suitability of Controllers	04/2016
GR-7.4 Approval Process	04/2016
GR-8 Close Links	
GR-8.1 Key Provisions	04/2016
GR-8.2 Definition of Close Links	04/2016
GR-8.3 Assessment Criteria	04/2016
GR-9 Cessation of Business	
GR-9.1 CBB Approval	04/2020
GR-10 Customer Complaints Procedures	
GR-10.1 General Requirements	12/2018
GR-10.2 Documenting Customer Complaints Handling Procedures	12/2018
GR-10.3 Procedures for Effective Handling of Complaints	04/2020
GR-10.4 Internal Complaint Handling Procedures	12/2018
GR-10.5 Response to Complaints	04/2020
GR-10.6 Records of Complaints	12/2018
GR-10.7 Reporting of Complaints	04/2020
GR-10.8 Monitoring and Enforcement	12/2018
GR-11 Outsourcing	
GR-11.1 Outsourcing	07/2022
GR-12 Information Security	
GR-12.1 Electronic Frauds	xx/2023
GR-12.2 Cyber security Risk Management	10/2022
GR-13 Fees and Charges	
GR-13.1 Merchant Fees on Payments to Zakat and Charity Fund	04/2021
GR-14 Marketing of Financial Services	
GR-14.1 Arrangements relating to Regulated Services provided by PSPs	10/2022
GR-15 Client Money	
GR-15.1 Client Money Requirements	04/2023



MODULE	GR:	General Requirements
CHAPTER	GR-12:	Information Security

GR-12.1 Electronic Frauds

GR-12.1.1 PSPs must implement enhanced fraud monitoring of movements in customers' accounts to guard against electronic frauds using various tools and measures, such as limits in value, volume and velocity.

GR-12.1.2 PSPs must have in place customer awareness communications, pre and post onboarding process, using video calls, short videos or pop-up messages, to alert and warn natural persons using online channels or applications about the risk of electronic frauds, and emphasise the need to secure their personal credentials and not share them with anyone, online or offline.

Secure Authentication

GR-12.1.3 PSPs and crowdfunding platform operators must take appropriate measures to authenticate the identity and authorisation of customers when the customer accesses the online or digital platform or when a transaction is initiated on the platform. Licensees must, at a minimum, establish adequate security features for customer authentication including the use of at least two different elements out of the following three elements:

- (a) Knowledge (something only the user knows), such as pin or password;
- (b) Possession (something only the user possesses) such as mobile phone, smart watch, smart card or a token; and
- (c) Inherence (something the user is), such as fingerprint, facial recognition, voice patterns, DNA signature and iris format.

GR-12.1.4 For the purpose of Paragraph GR-12.1.3, licensees must ensure that the authentication elements are independent from each other, in that the breach of one does not compromise the reliability of the others and are sufficiently complex to prevent forgery.

GR-12.1.5 For the purposes of Subparagraph GR-12.1.3 (b), where a customer's mobile device is registered/marked as 'trusted' using knowledge, biometric or other authentication methods through the licensee's application, the use of such mobile device would be considered as meeting the 'possession' element for authentication of future access or transactions using that device.