

CUSTOMER RESPONSIBILITIES

1. Introduction

This Annex describes the general responsibilities of the Customer with respect to the Terminals provided by Payter to assist the Customer in ensuring safe use, prevention of fraud and compliance with related Card Scheme Rules.

2. Deployment and Activation

- 2.1. Before deployment and/or activation of the Terminals, the Customer must:
 - 2.1.1. configure the Terminals in accordance with the applicable configuration instructions provided for the Terminal. The applicable manual can be retrieved through your distributor;
 - 2.1.2. check for visible damage to the housing;
 - 2.1.3. not use the Terminal if it is damaged or covered with a non-standard sticker, report any damage/tampering as per clause [7] below. For reference images, please check the Payter website, section downloads;
 - 2.1.4. charge and/or connect the Terminal to the internet;
 - 2.1.5. verify the Payter logo shows up after turning on the Terminal;
 - 2.1.6. not use the Terminal if the logo does not appear, report as per clause [7] below;
 - 2.1.7. check whether an internet connection is established;
 - 2.1.8. verify with Payter that the Terminals are connected to the Terminal Management System;
 - 2.1.9. if applicable, check whether the amounts are set correctly in the Terminal;
 - 2.1.10. after extended storage a test transaction is recommended;
 - 2.1.11. when distributing the Terminals within your organisation update the inventory (list of Terminals) with Terminal locations and personnel authorised to operate the Terminals; and
 - 2.1.12. ensure proper training and instruction of all personnel operating the Terminals, and ensure compliance with this Annex.

3. Transactions and reconciliation

- 3.1. Payter does not have access to the Customer's merchant account and it is therefore the Customer's responsibility to reconcile the payments being made into the Customer's merchant account with the transactions processed by the Terminal and the acquiring bank. Notwithstanding this, in the event that the Customer identifies a discrepancy they must notify Payter immediately so that Payter can provide assistance if possible.
- 3.2. Payter recommends that the Customer checks their account and the Terminal Management System for transactions, connectivity of the Terminal and any error messages.

4. Usage and Management

- 4.1. The Customer must when operating and using the Terminals:
 - 4.1.1. ensure that the Terminal is kept and operated in a suitable environment (please check the User Manuals), used only for the purposes for which it is designed, and operated in a proper manner;
 - 4.1.2. make no alteration to the Terminal and do not remove any component(s) from the Terminal without the prior written consent of Payter;
 - 4.1.3. not, without the prior written consent of Payter, allow any third party to use the Terminal or submit transactions via the Terminal on behalf of a third party. The Terminal may only be used by the Customer to submit transactions to the payment service provider in its own name and for the business it registered for during the Customer registration process (if applicable); and
 - 4.1.4. comply with the relevant instructions for the Terminals, including in particular :
 - 4.1.4.1. the User Manual of the particular type of Terminal; and
 - 4.1.4.2. the installation guide for Terminals to ensure IP connectivity for the Terminals to enable proper functioning.

5. Battery and storage

- 5.1. The Apollo terminals are equipped with Li-Ion batteries to ensure the integrity of the Terminals even when not powered. To ensure security during the full lifetime of the Terminals, these batteries need to be recharged at regular intervals (at least once every three (3) months) to avoid fall back to the

back-up battery. When a Terminal has not been connected to the Terminal Management System for an extended period of time, the Customer will receive alerts through the Terminal Management System (if applicable) to charge the batteries.

- 5.2. **Please note:** Failure to charge the batteries when notified drastically reduces the shelf life of the Terminal and can result in tampering the Terminal. Subject to Payter's prior written approval, a tampered Terminal needs to be returned to Payter for analysis, possible replacement of the batteries, and key injection.

6. Security

- 6.1. For security reasons, Customers and their personnel must check Terminals regularly for:
 - 6.1.1. visible damage to the housing (do not use the Terminal if it is damaged or covered with a non-standard sticker. For reference images, please check the Payter website, section downloads); and
 - 6.1.2. unusual cables connected anywhere on the Terminal.
- 6.2. Customers must:
 - 6.2.1. verify the Payter logo shows up after turning on the Terminal;
 - 6.2.2. verify with Payter, the identity of any third party persons or maintenance personnel claiming to repair the Terminals, prior to granting them access to modify or troubleshoot Terminals;
 - 6.2.3. not install, replace, or return Terminals without prior written consent from Payter;
 - 6.2.4. be aware of suspicious behaviour around Terminals (for example, attempts by unknown persons to unplug or open the Terminals); and
 - 6.2.5. report suspicious behaviour and indications of Terminal tampering or substitution to appropriate personnel (for example, to a manager or security officer) and to Payter.
- 6.3. Customers should maintain Terminal inventory to ensure that the location of all Terminals is known and to confirm that none of the Terminals have been lost, stolen or substituted. Payter recommends enforcing procedures to perform visual Terminal integrity inspections on a weekly basis as well as before and after storage of the Terminals.
- 6.4. In case of any doubts, the Customer must not use the Terminal (or allow the Terminals to be used) and must contact Payter via the usual escalation channels.
- 6.5. The Customer must follow the Card Scheme Rules in operating the Terminals to submit point of sale transactions.
- 6.6. As far as applicable, the Customer must comply with PCI DSS security requirements imposed by the Card Scheme Rules in handling and using Terminals and on the acquirer's request fill out a self-assessment questionnaire ('SAQs') prescribed by the Card Scheme Rules under applicable PCI DSS regulations to confirm such compliance.

7. Faulty, lost, stolen, or damaged/tampered Terminals

- 7.1. In the event of loss, theft, damage, tampering or destruction of a Terminal, the Customer must inform Payter or the distributor immediately, and in no event more than 24 hours after discovery of the incident, by sending an email to support@payter.nl or contacting Payter via the usual escalation channels. The notification must provide a complete description of the incident, summarising all efforts undertaken and planned to investigate the incident and secure the information and Terminals at issue. The notification must also identify appropriate contacts of the Customer who will be reasonably available to Payter.
- 7.2. In the event of a hardware failure during the Warranty Period, please contact Payter or the local distributor.
- 7.3. The Customer must ensure a central point of contact manned by trained representatives of the Customer, and that this is available for all end users of the Terminals to assist in performing the above tasks which such end users cannot perform themselves without assistance. Only such designated trained key representatives of the Customer may contact Payter or the distributor to receive support with respect to the Terminals and the Support Services of Payter. For requesting support with respect to Terminals such representative must use the current contact details to submit the support request by email or ticketing tool, following the relevant procedures.