PAN-NORDIC CARD ASSOCIATION

Secure card acceptance in hotel environments

To prevent card fraud and the misuse of cardholder data[1], major card organisations such as Visa and MasterCard have developed a security standard (PCI DSS[2]).

The easiest way to comply with the requirements is to use approved products (card readers, payment terminals) and never store, process or transmit cardholder data in the systems you use (hotel systems, booking systems, etc.)

These instructions for secure card acceptance at hotels and similar businesses are applicable for Visa, MasterCard, American Express and Diners Club. They do not apply to virtual card numbers or single-use card numbers distributed by Online Travel Agents (OTA), etc.

Payment terminals

- Use only approved chip and PIN terminals

Manual entry of card data

- Never register or store clear-text card data in your own systems or IT environment[3].
- It is permitted to send and to store truncated card numbers. The first six and last four digits are the maximum number of digits that may be displayed (1234 56XX XXXX 1234).
- Registration may be carried out in an approved chip and PIN terminal or in a solution where the card number can be entered online via the Internet and stored safely at a certified payment service provider (PSP). The provider will protect the card data for you. In this document, the service is called web link.
- For guaranteed reservations and No Show[4] it is prohibited to receive or register CVV/CVC[5].
- It is not allowed to receive CVV/CVC for manual registration of advance deposits.

Handling card data from booking engines or another party

- Strive to never receive card data. Instead, retrieve information from the Online Travel Agent (booking engine[6]) only when needed.
- Paper (faxes, printouts, etc.) with card numbers should always be stored in a restricted, locked area. Ensure that only authorised personnel have access to the data in that area.
- Electronic storage of card numbers should only take place at a certified Payment Service Provider.
- It is not allowed to send card numbers in clear-text via e-mail. Card data received via e-mail should be deleted.

Web links for hotels and similar businesses

- A web link at a certified PSP can be used for registering and storing card data securely. It is possible to:
    - Store card data short-term for reservations
    - Register No Show
    - Register Advance deposits

---

[1] Information from payment cards, e.g. card number and expiry date
[2] Payment Card Industry Data Security Standard is an information security standard
[3] E-mail systems, PCs, servers, ECRs, booking systems, etc.
[4] Compensation for one night's accommodation if a cardholder fails to cancel a reservation or claim a room
[5] The three-digit security code printed on the back of the card.
[6] Hotel booking companies.