# Nautical Software Solution Cybersecurity Policy (August 2021)

After a review and analysis of increased cybersecurity concerns, Mshop Software Inc. d/b/a Nautical Software Solution (hereinafter “NSS“) has decided to upgrade its software programs. As part of these upgrades, NSS’s software programs will no longer provide customers with the option store certain confidential, sensitive, or personal customer data (hereinafter collectively “confidential consumer information”). Specifically, upcoming releases of all NSS software programs will no longer contain fields for a customer’s credit card number, driver’s license number, social security number or bank ID. Due to compliance and security requirements, NSS strictly prohibits entering any confidential consumer information in any NSS software product. Inclusion of such confidential consumer information in the note fields, unused fields designed for other data, or otherwise is in violation of NSS’s Cybersecurity Policy.

## NSS Software Upgrade

All NSS customers shall be required to upgrade their software to the latest version, **The Marina Program** (TMP) v.5.1; **Management Pro** (M-PRO) v.6.0; **Marine Service Shop** (M-SHOP) v.10.3. There is no cost to the customers for such upgrades. All earlier versions of any NSS software shall hereinafter be considered un-authorized versions of NSS’s software and shall no longer be supported by NSS.

TO THE FULLEST EXTENT PERMITTED BY LAW, IN NO EVENT SHALL NSS, ITS OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, AND/OR ITS REPRESENTATIVES BE LIABLE FOR ANY DIRECT, INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL, CONSEQUENTIAL DAMAGES OR ANY OTHER DAMAGES WHATSOEVER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF USE, DATA OR PROFITS, ARISING OUT OF OR IN ANY WAY CONNECTED WITH THE CONTINUED USE OF ANY PRIOR OR UNAUTHORIZED SOFTWARE VERSIONS, WHETHER BASED ON CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY, OR OTHERWISE.

Any continued use of prior versions of NSS software shall continue at the sole risk of the customer. NSS shall not be liable or responsible for any damages which may result as a consequence of a breach of any customer’s software and/or database.

## Storage Regulations

Credit Card processing companies have regulations in place which specifically forbid anyone from keeping a record of the credit card security code or any other information which may be contained on the credit card’s magnetic strip, including, but not limited to any “track data”. This information was never intended and should never be inputted or maintained in NSS’ software applications. Should you keep paper copies of any credit card authorizations for your records, be advised that you are required to cross out the 3- or 4-digit security or CVV code with a dark pen to make it unreadable.

Cybersecurity regulations require that all unencrypted personal data be removed from business computer networks. Data privacy, sometimes also referred to as information privacy, is an area of data protection that concerns the proper handling of sensitive data including, notably, personal data, but also other confidential data i.e., credit card number, driver’s license number, social security number and bank ID. Safeguarding your customers’ credit card information is more than just a requirement from your payment processing company; it is also just good business.

*If your data is encrypted, the following information may be stored:*

- PAN (Primary Account Number) (e.g., 16-digit number on front of card)
- Cardholder name (e.g., John Smith)
- Expiration date (e.g., 5/18)
- Service code (Note: You cannot see this data on a physical card because it resides in the magnetic stripe)

*The following information should NEVER be stored:*

- Sensitive authentication data (i.e., full magnetic stripe info)
- PIN
- PIN block (i.e., the encrypted PIN)
- Card validation value (CVV), also known as three/four-digit service code or card security code

## Encrypt Electronic Storage and Secure All Paper Records

In certain situations, such as for recurring and/or mail order business, you may want to keep a hard copy or electronic record of certain transactions. Always secure any hard copies of all data in a safe and secure location.  All electronic records should always be encrypted. NSS processing company partners are all PCI DSS-verified providers.

## Encrypt Your Phone Recordings

If you take orders over the phone and record those calls for any purpose, you may have an unintended database of confidential consumer information. As with electronic data, all recordings need to be encrypted and stored in a password-protected directory to guard against potential theft or misuse. You also need to be sure that there are not any software programs which may be attached to your system which may allow any unintended transfers of confidential consumer information, such as a criminal transferring credit card information via a text-to-speech technology.