

## Credit Card Data Retention Policy

1. Customer credit card information will be stored in “QuickBooks” invoicing software. It is not shared with any other service provider.
2. The “Quickbooks” software will reside on a computer that is NOT connected to the internet via cable or wireless connection. Credit card information is NEVER transmitted over the internet. Credit card transactions are conducted through a Verifone® credit card machine over a telephone line with a direct line to merchant services.
3. “Quickbooks” backup is performed weekly to a flashdrive, and then stored in a metal safe, with a secure combination known only by the administrator. This metal safe is offsite in a secured and monitored location. This makes the information unreadable except to the administrator. When flashdrives are replaced they are demagnetized to render them useless, then destroyed.
4. Credit card information stored in “Quickbooks” will remain in the software because our customers have ongoing business transactions. It is the customers responsibility to give us updated credit card information when the information becomes outdated or compromised. Software will be password protected and used by the administrator only. Access to “Quickbooks” is restricted from any employee.
5. Credit card information will be removed from the “Quickbooks” software for these reasons: 1. The customer requested it be removed. 2. The customer has not used our service for a while. 3. We delete the customer account.
6. Two part credit card slips are used to document the transaction for the customer which is accompanied by a receipt printed by the credit card machine . The first part goes to the customer, the second part remains with the business for documentation and confirmation purposes for 30 days offsite in a secured monitored location. At 30 days, if there are no disputes, the second part of the credit card slip is incinerated and monitored until it is completely destroyed. We save no paper. Any documentation received with an order that contains any credit card information, along with the credit card slips, is incinerated.
7. The area that contains the stand alone computer which holds the credit card information will remain inaccessible to visitors. It will be under lock and key, and monitored by a security system and/or video surveillance. Any security monitoring data will be held a minimum of 3 months.

Compiled and written by Jeff Andrews (administrator) for Northern Tails Sharpening Inc. This policy will protect the integrity of any and all credit card data received and stored in our business server. This server is a stand alone computer not connected to the internet.  
Adopted: 2/10/10