Security Policy Package for NEXSTAR FDN (NEXSTAR LEGACY FOUNDATION)

Instructions:

- This Security Policy package was designed specifically for NEXSTAR FDN (NEXSTAR LEGACY FOUNDATION), based on information you provided to us as you completed the Security Assessment. Because this policy is specific to NEXSTAR FDN (NEXSTAR LEGACY FOUNDATION), it should not be used by any other entity as a basis for its own security policy.
- There are two parts to this package:
  A. The first half describes the NEXSTAR FDN (NEXSTAR LEGACY FOUNDATION) Security Policy as it relates to managers and anyone responsible for keeping your business and computer systems safe and in operation. It should not be given out to general staff (or anyone else) to read.
  B. The second half is the NEXSTAR FDN (NEXSTAR LEGACY FOUNDATION) Security Policy for ALL staff, and should be printed out and displayed on a notice board where all staff can read it, (but where members of the public cannot). ALL staff members need to read it, and then sign the back page to show that they have read it, and understood it.
- This Security Policy package is intended to relate only to your systems and processes that are involved in processing, transmitting or storing credit or debit card information (your "Card Transaction System"). While the principles, steps and statements outlined and made in this policy may apply generally to other of your systems and processes that are not involved in card transactions, you should not assume this policy is sufficient to cover your entire business.
- Because this Security Policy package is specific to the Card Transaction System you described to us as you completed the Security Assessment, modifications to that system may require changes to this policy. If you modify your Card Transaction System, please update your responses to the Security Assessment and, for a period of one year, we will make the necessary changes to this Security Policy for free. An out-of-date security policy may give you advice that is no longer suitable, and put your security and compliance status at risk.

Having a formal security policy, and even following it perfectly, does NOT guarantee that NEXSTAR FDN (NEXSTAR LEGACY FOUNDATION) will not be damaged by hackers, an accident, or some other event. It DOES help you reduce your risk. If you feel that you need more detailed advice on security policies, or on how to implement them, please visit

http://www.pcirapidcomply.com, or contact an information security specialist in your area.

Security Policy for NEXSTAR FDN (NEXSTAR LEGACY FOUNDATION)

Instructions For Managers and System Administrators ONLY

This section of the document is for all staff with managerial responsibilities within NEXSTAR FDN (NEXSTAR LEGACY FOUNDATION) and all staff tasked with any security or technology responsibilities. It should not be distributed to other staff, or to anyone outside the company that does not have authorization and a clear need to know.

Controlling the Scope of PCI

These policies should be applied everywhere (to all computers, to all people, etc.) but they MUST in particular apply to any computers, devices, or records that are subject to PCI. Computers and other network devices are subject to PCI if they process, store, or transmit cardholder information (such as account numbers, names, etc.) OR IF THEY ARE CONNECTED TO ANY SUCH DEVICE. So, for example, ANY device connected to a Point of Sale (POS) terminal is definitely subject to PCI.

Complying with the PCI Data Security Standard

In addition to the specific policy elements described below, the company and all staff are required to make sure that at all times they act in accordance with all requirements of the latest version of the Payment Card Industry Data Security Standard.

Computers and Software

- No computers are to be used to store cardholder data (such credit card numbers or information read off a card's magnetic stripe).
- No computers are to be connected to any Point of Sale terminal (via cables, wireless, or anything else).
- No computers other than virtual terminals are to be used to process cardholder data (such credit card numbers).
- No computers other than virtual terminals are to be used to transmit or share cardholder data over any sort of network.

Information and Records Stored On Computers and Devices

- DO NOT record, copy, or store cardholder information (such as account numbers) on any computer, thumb-drive, CD, DVD, etc.This includes magnetic stripe information, and other information like the three-digit numbers printed on the signature panel of cards.
- It IS allowed to record the last 4 digits ONLY of an account number.
- NEVER, UNDER ANY CIRCUMSTANCES, record, copy, or store cardholder PINs ANYWHERE.

Physical copies of Records (Paper Records, Thumbdrives, CD, DVDs, etc.)

- Cardholder data shall be stored only if strictly necessary, and only for as long as necessary. Data that is prohibited by other parts of this security policy must not be stored at all.
- NEVER, UNDER ANY CIRCUMSTANCES, write down, record, copy, or store cardholder PINs ANYWHERE.
- DO NOT record, copy, or store the three-digit number printed on the signature panel of any card.
- All paper records of cardholder data, and all thumbdrives, CDs, DVDs, etc, holding cardholder data are to be treated like cash. They must be kept in a locked area and access to them must be tightly restricted.
- Staff access to cardholder data records must be on a 'need to know' basis.
- Never share cardholder records with anyone outside the company, or with anyone inside the company who does not have management approval to use those records.
- Paper records of cardholder data, and thumbdrives, CD, DVDs, etc, holding cardholder data must not be thrown out or re-used for other purposes. When you are finished with them, they must be destroyed via shredding, using a company or machine approved of by management.
- Paper records of cardholder data are to be destroyed via cross-cut shredding, incineration, or pulping after five years (or at a time determined by management), using a company or machine approved of by management.
- Electronic media such as thumbdrives, CDs, DVDs, etc, ever used to hold cardholder data are to be physically destroyed after five years (or at a time determined by management), using a company or machine approved of by management.

Transmitting Information and Records

- Cardholder information must never be sent outside the work network unless it is protected by encryption. That encryption can either be on the communications channel (like SSL version3 for the web), or on the data itself (such as PGP). It is NOT enough to use winzip.

Physical Security

- Physical access to all Point of Sale terminals is restricted to those who have formal management approval.
- All visits to company premises by non-staff must be managed to make sure that cardholder data is not threatened. This includes, but is not limited to, making sure that visitors do not interfere with sensitive systems, or have unsupervised access to sensitive data or systems.
- If it is ever possible for visitors to be mistaken for staff by other staff members, visitors shall be required to wear visitor's badges, with badges assigned, tracked, and collected at the end of a visit by a staff member who has been explicitly assigned responsibility for this process.

- If any visitors are ever given any access to sensitive data or systems, they shall be required to first enter their information in a visitor's log, with the information gathered to include their name, the company they represent, and the name of the staff member who is authorizing their access.
- Paper records or electronic records of cardholder information must be kept in a locked drawer or box inside a separate room (like a back office), and the door must be locked unless someone with formal management approval is in the room at the time.
- Paper records or electronic records of cardholder information must not be removed from the secure area without formal management approval and a formal record made.
- Paper records and media holding cardholder information must be inventoried.
- Physical access to paper records with cardholder information on them is restricted to those who have formal management approval.
- Physical access to each computer or network device must be restricted to those with a need to have such access.

Policies and Procedures

- Responsibility for updating and distributing this Security Policy shall be formally assigned to one or more specific individuals.
- The company shall each year conduct a security review to identify threats and vulnerabilities, and to produce a risk assessment based on that review.
- In the event of suspicious behavior, or a security problem, all staff are required to contact management immediately.
- The company security policy must be reviewed on at least an annual basis.
- The company security policy must be reviewed whenever a change is made to the company's handling of cardholder data. These changes can be to either the company technology environment, or business processes.
- Management shall create a formal Incident Response Plan, ready to be executed in case of a security incident. Responsibility for creating, documenting, updating and distributing this plan shall be formally assigned to one or more specific individuals.
- The above formal Incident Response Plan must be updated as appropriate whenever a staff-member that is responsible for carrying out any part of`your Incident Response Plan changes employment status in a way which affects the Incident Response Plan.
- The above formal Incident Response Plan must be tested at least annually, and updated as appropriate.
- The company must have a process in place to educate staff on security issues. This must include training at the time of hiring`and at least annually.
- All staff with access to cardholder account numbers must either be known to management and known to be of good character, or must be subject to a background check.
- A list of third-party service providers given access to cardholder data will be maintained, and it will be kept complete and up-to-date.
- A written agreement will be created and enforced to bind third-party service providers given access to cardholder data to be responsible for the security of all cardholder data

they deal with. It will include an acknowledgement by the service providers of their responsibility for securing the cardholder data.

- Proper due diligence will be exercised to ensure that service providers under consideration are PCI DSS compliant prior to engaging any service provider.
- A program to monitor service providers' PCI DSS compliance status will be maintained to ensure that cardholder data is shared only with service providers that are (and continue to be) PCI DSS compliant.

SECURITY POLICY
FOR NEXSTAR FDN (NEXSTAR LEGACY FOUNDATION)

ALL STAFF MUST READ THIS DOCUMENT, AND SIGN THE BACK PAGE TO INDICATE THAT THEY UNDERSTAND IT AND WILL FOLLOW IT.

It is absolutely critical that all staff actively protect customer cardholder information from thieves and hackers. This is a legal requirement, and a business requirement, and must not be ignored.

This document is the company security policy. It describes what staff should do, and what they should not do. All staff are required to have read this document, and follow its directions at all times. **Failure to do so will result in disciplinary action, up to and including immediate termination.**

General Notes

- These policies apply everywhere (to all computers, to all people, etc.) but apply particularly to any computers, devices or records involved with cardholder information such as account numbers, names, and so on.

Computers and Software

- No computers are to be used to store cardholder data (such credit card numbers or information read off a card's magnetic stripe).
- No other computers are to be connected to any Point of Sale terminal (via cables, wireless, or anything else).
- No computers other than virtual terminals are to be used to transmit or share cardholder data over any sort of network.

Information and Records Stored On Computers and Devices

- DO NOT record, copy, or store cardholder information (such as account numbers) on any computer, thumb-drive, CD, DVD, etc.This includes magnetic stripe information, and other information like the three-digit numbers printed on the signature panel of cards.
- It IS allowed to record the last 4 digits ONLY of an account number.
- NEVER, UNDER ANY CIRCUMSTANCES, record, copy, or store cardholder PINs ANYWHERE.

Physical copies of Records (Paper Records, Thumbdrives, CD, DVDs, etc.)

- Cardholder data shall be stored only if strictly necessary, and only for as long as necessary. Data that is prohibited by other parts of this security policy must not be stored at all.
- NEVER, UNDER ANY CIRCUMSTANCES, write down, record, copy, or store cardholder PINs ANYWHERE.
- DO NOT record, copy, or store the three-digit number printed on the signature panel of any card.
- All paper records of cardholder data, and all thumbdrives, CDs, DVDs, etc, holding cardholder data are to be treated like cash. They must be kept in a locked area and access to them must be tightly restricted.
- Paper records or electronic records of cardholder information must not be removed from the secure area without formal management approval and an formal record made.

- Never share cardholder records with anyone outside the company, or with anyone inside the company who does not have management approval to use those records.
- Paper records of cardholder data, and thumbdrives, CD, DVDs, etc, holding cardholder data must not be thrown out or re-used for other purposes. When you are finished with them, they must be destroyed via shredding, using a company or machine approved of by management.
- Paper records or thumbdrives, CD, DVDs, etc, of cardholder data are to be destroyed via shredding after five years, using a company or machine approved of by management.

Transmitting Information and Records

- Cardholder information must never be sent outside the work network unless it is protected by encryption. That encryption can either be on the communications channel (like SSL version3 for the web), or on the data itself (such as PGP). It is NOT enough to use winzip.

Physical Security

- Physical access to all Point of Sale terminals is restricted to those who have formal management approval.
- If you see anyone (staff-member or not) near a Point of Sale terminal who does not have approval, you are required to report it to management immediately.
- All visitors must either be in the presence of a staff member who is responsible for supervising them, or be wearing a visible vistor's badge. All unsupervised visitors who are not wearing a visible visitor's badge must be escorted away from sensitive systems such as computers or paper records, and reported to management immediately.
- Paper records or electronic records of cardholder information must be kept in a locked drawer or box inside a separate room (like a back office), and the door must be locked unless someone with formal management approval is in the room at the time.
- Physical access to paper records with cardholder information on them is restricted to those who have formal management approval.
- If you see anyone (staff-member or not) near such paper records who does not have approval, you are required to report it to management immediately.

Policies and Procedures

- In the event of suspicious behavior, or a security problem, contact management immediately.
- Management is required to have in place a formal incident management plan, ready to be executed in case of a security incident.

Final Comments

This document, and the requirements described in it, helps the company in several important ways:

1. it reduces the chance that the company will be damaged by hackers or thieves.

2. it reduces the chance that customer information will be stolen, and so reduces the chance that the company will be sued.
3. it helps the company comply with an industry standard called the Payment Card Industry Data Security Standard (PCI DSS). Failure to do so can result in large fines, and the termination of the company's credit card processing services.
4. it reduces the chance that customer information will be stolen, and so reduces the chance that the company will be sued.

If you have any questions or comments about this policy, or about security issues, ask your manager.

I have read and understood this policy document, and agree to follow it.

Name	Signature	Date