# AGENDA – QUARTERLY MEETING of the NEBRASKA BRAND COMMITTEE

**Wednesday December 1, 2021**
**9:00 a.m. Central Time**
**Location of Meeting**
**Nebraska Beef Council**
**Meeting Room**
**1319 Central Ave.**
**Kearney, NE 68847**

**Online meeting credentials available via WebEx by registration only.**
**Email Danna.Schwenk@nebraska.gov for invitation prior to meeting start time.**

*All agenda items are for discussion and action will be taken as deemed appropriate. The Committee reserves the right to go into closed session in accordance with Neb.Rev.Stat. §84-1410.*

## Call to Order

- Pursuant to Neb.Rev.Stat. §84-1412(8) a current copy of the Nebraska Open Meetings Act is posted in the meeting room at a location accessible to members of the public.

- Roll Call

- **Adoption of Agenda**

- **Current Business**

1. Introduction of Attendees

2. Approval of September 8, 2021 & November 16th Meeting Minutes

3. Consideration and Acceptance of Financial Statements (Becki Vineyard)

4. 2022 Quarterly Meeting Date Schedule

5. Nebraska Brand Committee Policy, Rules and Regulations Review and Updates (Becki Vineyard)
    a. PCI Training
    b. Referral Bonuses

6. Staff Updates and Ratification of Personnel Changes
    a. Discussion on West Area Staff changes. (Leadership Team)

7. Estray Reports (Dean Anderson)

8. Strategic Plan Review

9. Fee Schedule Review and Discussion
    a. Brand Research Fee & Implementation Date (LB 572)

10. Technology Report (Danna Schwenk)
    a. E-Inspection Sub Committee
    b. December 1st report to Ag Committee
    c. December 9th presentation to Ag Committee

**11. Public Comment on E-Inspection**

12. Chief Investigators Report (Tom Hughson)

13. Chief Inspectors Report (Dean Anderson)

14. Registered Feedlot Audit Updates (Dean & Tom)

15. Executive Session: To Receive Legal Advice Related to Potential or Anticipated Litigation, Legislative, Personnel matters and Review of Special Projects

16. Clarification of the Committees interpretation of brand inspection requirements under the Registered Feedlot Program.

17. Executive Directors Report (John Widdowson)

18. **Public Comment**

19. **Adjournment**

**NEBRASKA BRAND COMMITTEE**

Post Office Box I • 411 Niobrara Ave.
Alliance, NE USA 69301-0775

**INSPECT • RECORD • POLICE**

November 9, 2021

# PUBLIC NOTICE

The regularly scheduled quarterly meeting of the Nebraska Brand Committee has been called by Chairman Adam Sawyer and is scheduled for Wednesday December 1, 2021 starting at 9:00 a. m. CST.

**Location of Meeting:**
**Nebraska Beef Council**
**Meeting Room**
**1319 Central Ave**
**Kearney, NE 68847**

An agenda and one copy of all documents to be considered are available for inspection at the headquarters office of the Nebraska Brand Committee, 411 Niobrara Ave., Alliance NE 69301 or upon request by calling the Nebraska Brand Committee at (308) 763-2930. In accordance with the Americans with Disabilities Act, reasonable accommodations will be provided to persons with disabilities. If you require reasonable accommodations to attend, please call (308) 763-2930 to coordinate necessary arrangements.

John Widdowson
Executive Director

**September 8, 2021**

## Minutes – QUARTERLY MEETING of the NEBRASKA BRAND COMMITTEE

**Wednesday September 8, 2021**
**10:00 a.m. Central Time**
**Location of Meeting**
**Upper Loup NRD**
**Meeting Room**
**39252 Hwy 2**
**Thedford, NE 69166**

### Call to Order

Meeting was called to order by Chairman Sawyer at 10:05 am

- Pursuant to Neb.Rev.Stat. §84-1412(8) a current copy of the Nebraska Open Meetings Act is posted in the meeting room at a location accessible to members of the public. Open meetings act was read by Chairman Sawyer

- Roll Call

  Adam Sawyer- Present
  Terry Cone- Present
  Chris Gentry- Present
  Tanya Storer- Present (arrived at 10:42 a.m.)
  Duane Gangwish- Present

- **Adoption of Agenda**
  Duane Gangwish moved to accept the agenda as presented
  Terry Cone seconded the motion
  No discussion
  Adam Sawyer- Yes
  Terry Cone- Yes
  Chris Gentry- Yes
  Duane Gangwish- Yes
  Motion passed

- **Current Business**

1. Introduction of Attendees
2. Adam Sawyer Chairman
3. Terry Cone Committee Member

| | |
|---|---|
| 4. Chris Gentry | Committee Member |
| 5. Tanya Storer | Committee Member |
| 6. Duane Gangwish | Committee Member |
| 7. John Widdowson | Director |
| 8. Dave Horton | Chief Investigator |
| 9. Thomas Hughson | Investigator |
| 10. Brent Deibler | Investigator |
| 11. Christian Fell | Investigator |
| 12. Kayla Jesse | Area supervisor |
| 13. Kortnie Shafer | Area Supervisor via WebEx |
| 14. Shawn Hanks | Area super Visor |
| 15. Cody Waite | Area Supervisor via WebEx |
| 16. Danna Schwenk | IT Coordinator |
| 17. Becki Vineyard | HR Head, Office Manager |
| 18. Dean Anderson | Business Operations Manager |
| 19. Jacob Leaver | State Budget Office |
| 20. Spike Jordan | via WebEx |
| 21. Jay Ferris | via WebEx |
| 22. Clint Varner | State Budget via WebEx |
| 23. Melody Benjamin | |

2. Approval of June 15, 2021 Meeting Minutes

Chris Gentry moved to approve the minutes as read
Adam Sawyer Seconded the motion
No Discussion
Adam Sawyer- Yes
Terry Cone- Yes
Chris Gentry- Yes
Duane Gangwish- Yes
Motion passed

3. Consideration and Acceptance of Financial Statements

John Widdowson and Becki Vineyard presented the financial statements and future budget plans. Thanked Jacob Leaver for attending and his guidance moving forward.

Terry Cone moved to accept the financial statements
Chris Gentry seconded the motion
No Discussion
Adam Sawyer- Yes
Terry Cone- Yes
Chris Gentry- Yes
Tanya Storer- Abstain
Duane Gangwish- Yes
Motion passed

4. Election of Chairman and Vice Chairman per NE Statute 54-191.

Chairman Sawyer opened the floor to nominations for Chairman
Chris Gentry nominated Adam Sawyer
Duane Gangwish seconded the nomination
No other nominations
Roll called
No Discussion
Adam Sawyer- Yes
Terry Cone- Yes
Chris Gentry- Yes
Tanya Storer- Yes
Duane Gangwish- Yes
Adam Sawyer is confirmed as Chairman
Chairman Sawyer opened the floor to nominations for vice chair

Adam Sawyer nominated Terry Cone
Duane Gangwish seconded the nomination
No other nominations
Roll Called
No Discussion
Adam Sawyer- Yes
Terry Cone- Yes
Chris Gentry- Yes
Tanya Storer- Yes
Duane Gangwish- Yes
Terry Cone is confirmed as Vice Chair.

5. Brand Recording Issue (Woodward)
John Widdowson and Dave Horton explained that a brand was double issued due to an error while transferring computer systems. Mista White joined the meeting by telephone to clarify the issue.
Adam Sawyer moved to revoke brand 41446.00
Terry Cone seconded the motion
No Discussion
Adam Sawyer- Yes
Terry Cone- Yes
Chris Gentry- Yes
Tanya Storer- Yes
Duane Gangwish- Yes
Motion passed
The Committee requested that the Chief Investigator communicate with the people whose brand was revoked and to address how to handle any cattle that may have been branded with this brand while it was in their possession.

6. Nebraska Brand Committee Policy, Rules and Regulations Review and Updates
John Widdowson and Becki Vineyard presented the new 48-hour notice for brand inspection, policy for the Committee's consideration and approval.

Chairman Sawyer moved to approve the 48-hour notice policy
Duane Gangwish seconded the motion
No Discussion
Adam Sawyer- Yes
Terry Cone- Yes
Chris Gentry- Yes
Tanya Storer- Yes
Duane Gangwish- Yes
Motion passed

7. Legislative Updates

John Widdowson presented the roll out schedule for LB572 and discussed meetings he will be having with senators about the roll out and its progress. Thomas Hughson discussed the timetable for the use of waivable citations by the investigators

No action taken by the Committee

8. Staff Updates and Ratification of Personnel changes

Becki Vineyard presented the personnel changes for the past quarter
Chris Gentry moved to ratify the personnel changes
Duane Gangwish seconded the motion
No Discussion
Adam Sawyer- Yes
Terry Cone- Yes
Chris Gentry- Yes
Tanya Storer- Yes
Duane Gangwish- Yes
Motion passed

9. Estray Reports

There were no school funds disbursed this quarter for the Committee to review.
No action taken

10.. Strategic Plan Review

Chairman Sawyer and John Widdowson discussed the strategic plan and its history.
No action was taken

11. Fee Schedule Review and Discussion

John Widdowson presented the pluses and minuses of raising recording fees and the desire to spend down the cash equity fund to a reasonable and prudent balances.
No action taken

12. Executive Session:

Terry Cone moved to move into executive session for the protection of the public interest to receive privileged and confidential legal advice relating to potential and actual litigation, to discuss negotiation strategy relating to legislative developments, and to discuss confidential personnel matters.

Duane Gangwish seconded the motion

No Discussion

Adam Sawyer- Yes
Terry Cone- Yes
Chris Gentry- Yes
Tanya Storer- Yes
Duane Gangwish- Yes

Motion passed

Committee moved into executive session at 12:25 p.m.

The Committee came back into open session and the public was permitted to return at 1:58 p.m.

Tanya Storer moved to come out of executive session
Duane Gangwish seconded the motion

No Discussion

Adam Sawyer- Yes
Terry Cone- Yes
Chris Gentry- Yes
Tanya Storer- Yes
Duane Gangwish- Yes

Motion passed

13. Technology Report (IT Coordinator Danna Schwenk)

Danna Schwenk summarized her written report

14. Investigators Reports

A. Tom Hughson summarized his written report
B. C J Fell summarized his written report
C. Brent Deibler summarized his written report

15. District Supervisors Reports

A. Kortnie Shaffer summarized his written report
B. Cody Waite summarized her written report
C. Shawn Hanks summarized his written report
D. Kayla Jesse summarized her written report

16. Registered Feedlot Audit Updates

Dave Horton gave a brief update on the completion of audits

17. Chief Investigator's Report.

Dave Horton summarized his written report

18. Executive Directors Report.

John Widdowson provided a summary of his work and efforts over the past months

19. **Public Comment**

Public comment was given by Melody Benjamin and Spike Jordan

20. **Adjournment**

Tanya Storer moved to adjourn the meeting

Chris Gentry seconded the motion

No Discussion

Adam Sawyer- Yes
Terry Cone- Yes
Chris Gentry- Yes
Tanya Storer- Yes
Duane Gangwish- Yes

Motion passed

Meeting Adjourned at 3:45pm

## Minutes – SPECIAL MEETING of the NEBRASKA BRAND COMMITTEE

**Tuesday, November 16, 2021**
**8:30 a.m. Central Time / 7:30 a.m. Mountain Time**

**Via Telecommunications**
**Conference Call Access Number: (408) 418-9388**
**-OR-**
**Video Link:**
https://sonvideo.webex.com/sonvideo/j.php?MTID=mf5cb17fd6a80d1161ebcb36149a1a01b
**Meeting Code:** 2484 626 2556
**Password: Brand**

### Call to Order

The meeting was called to order by Chairman Sawyer at 8:33 a.m. CT

- The public meeting statement was read by Chairman Sawyer

- **Roll Call**

| | |
|---|---|
| Adam Sawyer | Present |
| Terry Cone | Present |
| Chris Gentry | Present (arrived 8:44 a.m. left at 9:04 a.m. due to technical difficulties) |
| Tanya Storer | Present |
| Duane Gangwish | Present |

- **Adoption of Agenda**

Duane Gangwish moved to adopt the agenda as presented
Terry Cone seconded the motion
No discussion

Adam Sawyer Yes
Terry Cone Yes
Chris Gentry Not Present
Tanya Storer Yes
Duane Gangwish Yes
Motion Passed

- **Current Business**

1. Introduction of Attendees.
   Adam Sawyer
   Chris Gentry
   Tanya Storer
   Terry Cone
   Duane Gangwish
   John Widdowson
   Danna Schwenk
   Dean Anderson
   Tom Hughson
   Becki Vineyard
   Mark Fahleson
   Spike Jordan
   Marie Farr
   Melody Benjamin
   Jim Dinklage
   Casey Shoemaker
   Ashlin Bussell
   Mikala Walker
   Tracy Bradley
   Steve Erdman
   Martian Swane
   Kensy Johnston
   Denis Child
   Brenda Mashek

2. Review and discussion of EID Subgroup meetings.

   Chris Gentry moved to make all future EID working group meetings open to the public.

   Tanya Storer seconded the motion.

   Discussion among Committee members occurred.

   Terry Cone discussed, among other things, that these meetings were a working group that included consideration of proprietary information provided by industry officials and vendors that they may not want to share with the public as it may result in a competitive disadvantage. Because the working group has no authority to make any decisions and no action is taken at these meetings, the group should be permitted to gather information and evaluate the issues without a formal public meeting.

Chris Gentry stated that he felt the Committee decided the process should be 100 percent transparent and this necessitates having the working group's meetings open to the public.

Tanya Storer stated that transparency is key to this process. She further questioned whether anything proprietary would be disclosed or discussed and wants to keep the process as transparent as possible.

Adam Sawyer gave some background on the idea that the subgroup meetings would bring together a small group of producers and industry representatives to gather information and evaluate what would work and what would not work in the field, with all of that to be reported back to the full Committee at an open public meeting. By having all of the information gathering and evaluation subject to an open public meeting, there is a risk that some may think these ideas represent a decided direction rather than just idea. Chairman Sawyer asked Special Appointed Attorney General Mark Fahleson to explain it from a legal standpoint.

Mark Fahleson stated that because no quorum of the Committee is present at any subgroup meeting, because the subgroup is not authorized to make any policy and cannot take any formal action on behalf of the Committee, the subgroup meetings are not subject to the Nebraska Open Meetings Act. However, the Committee, should it so decide, could decide to treat the subgroup meetings as public meetings.

Duane Gangwish stated that the law allows for small groups to meet and gather information to report back to the Committee so long as a quorum of the Committee is not present and the subgroup is not taking any action for the Committee. Producers form all sectors will give a recommendation to the Committee. It is his opinion that the group should not be public at this time so as to not hamper the free and full discussion of ideas.

Tanya Storer said she feels there is a lack of transparency if the subgroup meetings are not open to the public.

Roll Called

| | |
|---|---|
| Adam Sawyer | No |
| Terry Cone | No |
| Chris Gentry | Yes |
| Tanya Storer | Yes |
| Duane Gangwish | No |

Motion failed.

3. Consideration of formal policy relating to conduct of meetings of the EID Subgroup. No action taken based on previous vote.

- **Adjournment**

  Tanya Storer moved to adjourn the meeting.
  Duane Gangwish seconded the motion

  Roll Called

| | |
|---|---|
| Adam Sawyer | Yes |
| Terry Cone | Yes |
| Chris Gentry | Not Present |
| Tanya Storer | Yes |
| Duane Gangwish | Yes |

  Motion Passed

Meeting adjourned at 9:06 a.m.

STATE OF NEBRASKA
Fund Summary By Fund
Secure Version - Prior Month
As of September 30, 2021

Agency Number 039 NEBR BRAND COMMITTEE
Agency Division
Fund 23910 BRND INSP & THEFT PR

| | ACCOUNT CODE AND DESCRIPTION | | DEBIT CURRENT MONTH | CREDIT CURRENT MONTH | ACCOUNT BALANCE DEBIT | ACCOUNT BALANCE CREDIT |
|---|---|---|---|---|---|---|
| Assets | 100000 | Assets | | | | |
| | 111100 | GENERAL CASH | 108,546.52 | | 2,871,090.41 | |
| | 112200 | DEPOSITS WITH VENDORS | | | 637.71 | |
| | 132900 | NSF ITEMS SUSPENSE | | | 50.00 | |
| | 139901 | AR INVOICED (SYSTEM) | | | 189.00 | |
| | | Fund 23910 Assets Total | 108,546.52 | | 2,871,967.12 | |
| Liabilities | 200000 | Liabilities | | | | |
| | 211700 | REC'D - NOT VOUCHERED (S | | | | 12,213.84 |
| | 211900 | AAI DUE TO VENDOR (SYSTE | | 4,088.79- | | 6,446.19 |
| | 215100 | DUE TO FUND - SHORT TERM | | | | 22.39- |
| | | Fund 23910 Liabilities Total | | 4,088.79- | | 18,637.64 |
| Fund Equity | 300000 | Fund Equity | | | | |
| | 349100 | UNDESIGNATED | | | | 3,030,954.60 |
| | | Fund 23910 Fund Equity Total | | | | 3,030,954.60 |
| Revenues | 470000 | Revenues - Sales & Charges | | | | |
| | 474100 | GENERAL BUSINESS FEES | | 163,963.00 | | 386,108.00 |
| | 474101 | SURCHARGE | | 20,704.92 | | 51,215.51 |
| | 474102 | Auction Markets | | 75,734.00 | | 201,067.00 |
| | 474103 | PACKING HOUSE | | 34,128.00 | | 135,689.00 |
| | 474104 | RFL REGISTERED FED LOTS | | 207,750.00 | | 313,500.00 |
| | 474106 | LATE NOTICE SURCHARGE | | 50.00 | | 50.00 |
| | 474108 | EXPIRED AND REINSTATED | | 1,490.00 | | 13,070.00 |
| | 474109 | ADD FREEZE | | 75.00 | | 250.00 |
| | 474110 | ADD LOCATION | | 60.00 | | 150.00 |
| | 474111 | Brand Lease | | 1.00 | | 2.00 |
| | 474112 | BRANDS-NEW | | 6,110.00 | | 12,510.00 |
| | 474113 | BRANDS-RENEWAL | | 18,950.00 | | 79,050.00 |
| | 474114 | BRANDS-TRANSFER | | 2,320.00 | | 5,880.00 |
| | 474115 | BRANDS-DUPLICATE CERTIFIC | | 1.00 | | 1.00 |
| | 474116 | GRAZING PERMITS | | | | 30.00 |
| | 474118 | OUT-OF-STATE BRANDING PERMIT | | 50.00 | | 50.00 |
| | | Major Account 470000 Total | | 531,386.92 | | 1,198,622.51 |
| Revenues | 480000 | Revenues - Miscellaneous | | | | |
| | 481100 | INVESTMENT INCOME | | 3,280.09 | | 10,593.20 |
| | 484500 | REIMB NON-GOVT SOURCES | | 4,347.04 | | 6,520.18 |
| | 486600 | CREDIT CARD CLEARING | | 1,099.65 | | 17,488.98 |
| | | Major Account 480000 Total | | 8,726.78 | | 34,602.36 |
| | | Fund 23910 Revenues Total | | 540,113.70 | | 1,233,224.87 |

Agency Number 039 NEBR BRAND COMMITTEE
Agency Division
Fund 23910 BRND INSP & THEFT PR

| | ACCOUNT CODE AND DESCRIPTION | | DEBIT CURRENT MONTH | CREDIT CURRENT MONTH | ACCOUNT BALANCE DEBIT | ACCOUNT BALANCE CREDIT |
|---|---|---|---|---|---|---|
| Expenditures | 510000 | Personal Services | | | | |
| | 511100 | PERMANENT SALARIES-WAGES | 185,615.36 | | 537,846.83 | |
| | 511106 | INTERMITTENT SALARIES | 26,531.01 | | 67,998.22 | |
| | 511700 | EMPLOYEE BONUSES | 1,140.00 | | 3,650.00 | |
| | 511800 | COMPENSATORY TIME PAID | 11,931.53 | | 51,074.47 | |
| | 512100 | VACATION LEAVE EXPENSE | 11,505.74 | | 20,856.73 | |
| | 512200 | SICK LEAVE EXPENSE | 10,167.63 | | 17,586.54 | |
| | 512300 | HOLIDAY LEAVE EXPENSE | 128.34 | | 29,134.92 | |
| | 512500 | FUNERAL LEAVE EXPENSE | 753.62 | | 1,177.98 | |
| | 515100 | RETIREMENT PLANS EXPENSE | 16,481.31 | | 49,247.11 | |
| | 515200 | FICA EXPENSE | 17,721.12 | | 52,005.40 | |
| | 515400 | LIFE & ACCIDENT INS EXP | .48- | | | |
| | 515500 | HEALTH INSURANCE EXPENSE | 49,188.24 | | 151,502.90 | |
| | 516300 | EMPLOYEE ASSISTANCE PRO | | | 716.88 | |
| | 516500 | WORKERS COMP PREMIUMS | | | 36,023.00 | |
| | | Major Account 510000 Total | 331,163.42 | | 1,018,820.98 | |
| Expenditures | 520000 | Operating Expenses | | | | |
| | 521100 | POSTAGE EXPENSE | 61.77 | | 2,203.64 | |
| | 521300 | FREIGHT EXPENSE | | | 602.37 | |
| | 521400 | CIO CHARGES | 14,355.64 | | 44,715.17 | |
| | 521500 | PUBLICATION & PRINT EXP | | | 5,384.97 | |
| | 521900 | AWARDS EXPENSE | 83.29 | | 226.55 | |
| | 522100 | DUES & SUBSCRIPTION EXP | 78.00 | | 1,466.42 | |
| | 522200 | CONFERENCE REGISTRATION | | | 2,185.00 | |
| | 523201 | NATURAL GAS | 36.33 | | 79.65 | |
| | 523202 | ELECTRICITY | 331.42 | | 1,051.77 | |
| | 523203 | WATER | 23.07 | | 208.24 | |
| | 523204 | SEWER | 4.66 | | 13.98 | |
| | 524600 | RENT EXPENSE-BUILDINGS | 1,416.99 | | 4,250.97 | |
| | 525100 | RENT EXP-OFFICE EQUIP | | | 597.00 | |
| | 526100 | REP & MAINT-REAL PROPERT | 37.43 | | 12,422.27 | |
| | 527200 | REP & MAINT-MOTOR VEHICL | 2,126.00 | | 3,057.14 | |
| | 531100 | OFFICE SUPPLIES EXPENSE | 415.30 | | 7,507.22 | |
| | 532200 | PERSONAL COMPUTING EQUIPMENT | | | 305.41 | |
| | 534800 | CONST & MAINT SUP EXP | | | 16.75 | |
| | 538185 | GASOLINE | 1,672.37 | | 4,717.07 | |
| | 541100 | ACCTG & AUDITING SERVICES | 27,598.06 | | 69,221.94 | |
| | 541500 | LEGAL SERVICES EXPENSE | 445.00 | | 3,350.00 | |
| | 541700 | LEGAL RELATED EXPENSE | | | 30.00 | |
| | 547100 | EDUCATIONAL SERVICES | | | 560.00 | |

STATE OF NEBRASKA

Fund Summary By Fund

Secure Version - Prior Month

As of September 30, 2021

Agency Number 039 NEBR BRAND COMMITTEE

Agency Division

Fund 23910 BRND INSP & THEFT PR

| | ACCOUNT CODE AND DESCRIPTION | DEBIT CURRENT MONTH | CREDIT CURRENT MONTH | ACCOUNT BALANCE DEBIT | ACCOUNT BALANCE CREDIT |
|---|---|---|---|---|---|
| Expenditures | 520000 Operating Expenses | | | | |
| | 548500 LAWN/LANDSCAPE/SNOW REMOVAL | | | 368.00 | |
| | 548700 REFUSE/RECYCLING | 45.50 | | 182.00 | |
| | 548900 WEED CONTROL | 230.00 | | 275.00 | |
| | 549200 JANITORIAL/SECURITY SRVS | 58.59 | | 175.77 | |
| | 555200 SOFTWARE - NEW PURCHASES | | | 2,400.00 | |
| | 556100 INSURANCE EXPENSE | | | 2,474.00 | |
| | 556300 SURETY & NOTARY BONDS | | | 44.00 | |
| | 559100 OTHER OPERATING EXP | 319.61 | | 5,292.48 | |
| | Major Account 520000 Total | 49,339.03 | | 175,384.78 | |
| Expenditures | 570000 Travel Expenses | | | | |
| | 571100 LODGING | 1,039.99 | | 10,106.98 | |
| | 571600 MEALS - TAXABLE | 180.15 | | 1,942.14 | |
| | 571800 MEALS - TRAVEL STATUS | 490.76 | | 2,147.40 | |
| | 572100 COMMERCIAL TRANSPORTATIO | | | 276.80 | |
| | 574500 PERSONAL VEHICLE MILEAGE | 45,265.04 | | 120,195.17 | |
| | 575100 MISC TRAVEL EXPENSE | | | 110.00 | |
| | Major Account 570000 Total | 46,975.94 | | 134,778.49 | |
| Expenditures | 580000 Capital Outlay | | | | |
| | 581500 IMPROVEMENTS TO BUILDINGS | | | 13,659.74 | |
| | 584200 VEHICLES & VEHICLE EQ | | | 68,206.00 | |
| | Major Account 580000 Total | | | 81,865.74 | |
| | Fund 23910 Expenditures Total | 427,478.39 | | 1,410,849.99 | |
| | Fund 23910 Total | 536,024.91 | 536,024.91 | 4,282,817.11 | 4,282,817.11 |

STATE OF NEBRASKA

Fund Summary By Fund

Secure Version - Prior Month

As of September 30, 2021

Agency Number 039 NEBR BRAND COMMITTEE

Agency Division

Fund 73910 ESTRAY FUND

| | ACCOUNT CODE AND DESCRIPTION | | DEBIT CURRENT MONTH | CREDIT CURRENT MONTH | ACCOUNT BALANCE DEBIT | ACCOUNT BALANCE CREDIT |
|---|---|---|---|---|---|---|
| Assets | 100000 | Assets | | | | |
| | 111100 | GENERAL CASH | 5,340.34 | | 94,157.14 | |
| | | Fund 73910 Assets Total | 5,340.34 | | 94,157.14 | |
| Liabilities | 200000 | Liabilities | | | | |
| | 214101 | ESTRAY DEPOSITS | | 5,239.36 | | 84,119.02 |
| | 215100 | DUE TO FUND - SHORT TERM | | 100.98 | | 10,038.12 |
| | | Fund 73910 Liabilities Total | | 5,340.34 | | 94,157.14 |
| | | Fund 73910 Total | 5,340.34 | 5,340.34 | 94,157.14 | 94,157.14 |

Fund Summary By Fund
Menu Version
As of October 31, 2021

Agency Number 039 NEBR BRAND COMMITTEE
Agency Division
Fund 23910 BRND INSP & THEFT PR

| | ACCOUNT CODE AND DESCRIPTION | | DEBIT CURRENT MONTH | CREDIT CURRENT MONTH | ACCOUNT BALANCE DEBIT | ACCOUNT BALANCE CREDIT |
|---|---|---|---|---|---|---|
| Revenues | 470000 | Revenues - Sales & Charges | | | | |
| | 474100 | GENERAL BUSINESS FEES | | 187,820.05 | | 573,928.05 |
| | 474101 | SURCHARGE | | 28,529.24 | | 79,744.75 |
| | 474102 | Auction Markets | | 84,326.00 | | 285,393.00 |
| | 474103 | PACKING HOUSE | | 39,731.00 | | 175,420.00 |
| | 474104 | RFL REGISTERED FED LOTS | | 27,200.00 | | 340,700.00 |
| | 474106 | LATE NOTICE SURCHARGE | | 1,000.00 | | 1,050.00 |
| | 474108 | EXPIRED AND REINSTATED | | 6,950.00 | | 20,020.00 |
| | 474109 | ADD FREEZE | | | | 250.00 |
| | 474110 | ADD LOCATION | | 60.00 | | 210.00 |
| | 474111 | Brand Lease | | 4.00 | | 6.00 |
| | 474112 | BRANDS-NEW | | 5,200.00 | | 17,710.00 |
| | 474113 | BRANDS-RENEWAL | | 4,800.00 | | 83,850.00 |
| | 474114 | BRANDS-TRANSFER | | 1,760.00 | | 7,640.00 |
| | 474115 | BRANDS-DUPLICATE CERTIFIC | | | | 1.00 |
| | 474116 | GRAZING PERMITS | | 45.00 | | 75.00 |
| | 474118 | OUT-OF-STATE BRANDING PERMIT | | 50.00 | | 100.00 |
| | | Major Account 470000 Total | | 387,475.29 | | 1,586,097.80 |
| Revenues | 480000 | Revenues - Miscellaneous | | | | |
| | 481100 | INVESTMENT INCOME | | 3,602.63 | | 14,195.83 |
| | 484500 | REIMB NON-GOVT SOURCES | | 4,777.23 | | 11,297.41 |
| | 486600 | CREDIT CARD CLEARING | | 19,057.98- | | 1,569.00- |
| | | Major Account 480000 Total | | 10,678.12- | | 23,924.24 |
| Revenues | 490000 | Other Financing Sources | | | | |
| | 491300 | SALE - SURP PROP/FIXED ASSET | | 9.20 | | 9.20 |
| | | Major Account 490000 Total | | 9.20 | | 9.20 |
| | | Fund 23910 Revenues Total | | 376,806.37 | | 1,610,031.24 |
| Expenditures | 510000 | Personal Services | | | | |
| | 511100 | PERMANENT SALARIES-WAGES | 195,176.28 | | 733,023.11 | |
| | 511106 | INTERMITTENT SALARIES | 30,097.20 | | 98,095.42 | |
| | 511700 | EMPLOYEE BONUSES | 1,150.00 | | 4,800.00 | |
| | 511800 | COMPENSATORY TIME PAID | 2,107.05 | | 53,181.52 | |
| | 512100 | VACATION LEAVE EXPENSE | 7,825.34 | | 28,682.07 | |
| | 512200 | SICK LEAVE EXPENSE | 751.76 | | 18,338.30 | |
| | 512300 | HOLIDAY LEAVE EXPENSE | 9,589.69 | | 38,724.61 | |
| | 512500 | FUNERAL LEAVE EXPENSE | | | 1,177.98 | |
| | 515100 | RETIREMENT PLANS EXPENSE | 16,132.99 | | 65,380.10 | |
| | 515200 | FICA EXPENSE | 17,564.73 | | 69,570.13 | |

Agency Number 039 NEBR BRAND COMMITTEE
Agency Division
Fund 23910 BRND INSP & THEFT PR

| | ACCOUNT CODE AND DESCRIPTION | | DEBIT CURRENT MONTH | CREDIT CURRENT MONTH | ACCOUNT BALANCE DEBIT | ACCOUNT BALANCE CREDIT |
|---|---|---|---|---|---|---|
| Expenditures | 510000 | Personal Services | | | | |
| | 515500 | HEALTH INSURANCE EXPENSE | 52,256.26 | | 203,759.16 | |
| | 516300 | EMPLOYEE ASSISTANCE PRO | | | 716.88 | |
| | 516500 | WORKERS COMP PREMIUMS | | | 36,023.00 | |
| | | Major Account 510000 Total | 332,651.30 | | 1,351,472.28 | |
| Expenditures | 520000 | Operating Expenses | | | | |
| | 521100 | POSTAGE EXPENSE | 1,301.35 | | 3,504.99 | |
| | 521300 | FREIGHT EXPENSE | 229.17 | | 831.54 | |
| | 521400 | CIO CHARGES | 14,206.87 | | 58,922.04 | |
| | 521500 | PUBLICATION & PRINT EXP | 210.00 | | 5,594.97 | |
| | 521900 | AWARDS EXPENSE | | | 226.55 | |
| | 522100 | DUES & SUBSCRIPTION EXP | 75.00 | | 1,541.42 | |
| | 522200 | CONFERENCE REGISTRATION | 400.00 | | 2,585.00 | |
| | 523201 | NATURAL GAS | 48.10 | | 127.75 | |
| | 523202 | ELECTRICITY | 293.95 | | 1,345.72 | |
| | 523203 | WATER | 84.41 | | 292.65 | |
| | 523204 | SEWER | 4.71 | | 18.69 | |
| | 524600 | RENT EXPENSE-BUILDINGS | 1,416.99 | | 5,667.96 | |
| | 525100 | RENT EXP-OFFICE EQUIP | 597.00 | | 1,194.00 | |
| | 526100 | REP & MAINT-REAL PROPERT | 60.39 | | 12,482.66 | |
| | 527200 | REP & MAINT-MOTOR VEHICL | | | 3,057.14 | |
| | 531100 | OFFICE SUPPLIES EXPENSE | 1,541.04 | | 9,048.26 | |
| | 532200 | PERSONAL COMPUTING EQUIPMENT | 3,161.86 | | 3,467.27 | |
| | 533132 | UNIFORMS | 3,515.84 | | 3,515.84 | |
| | 534800 | CONST & MAINT SUP EXP | | | 16.75 | |
| | 538185 | GASOLINE | 56.60 | | 4,773.67 | |
| | 541100 | ACCTG & AUDITING SERVICES | 18,868.48 | | 88,090.42 | |
| | 541500 | LEGAL SERVICES EXPENSE | 250.00 | | 3,600.00 | |
| | 541700 | LEGAL RELATED EXPENSE | | | 30.00 | |
| | 547100 | EDUCATIONAL SERVICES | | | 560.00 | |
| | 548500 | LAWN/LANDSCAPE/SNOW REMOVAL | | | 368.00 | |
| | 548700 | REFUSE/RECYCLING | 45.50 | | 227.50 | |
| | 548900 | WEED CONTROL | | | 275.00 | |
| | 549200 | JANITORIAL/SECURITY SRVS | 117.18 | | 292.95 | |
| | 555200 | SOFTWARE - NEW PURCHASES | | | 2,400.00 | |
| | 556100 | INSURANCE EXPENSE | | | 2,474.00 | |
| | 556300 | SURETY & NOTARY BONDS | | | 44.00 | |
| | 559100 | OTHER OPERATING EXP | 897.18 | | 6,189.66 | |
| | | Major Account 520000 Total | 47,381.62 | | 222,766.40 | |

Agency Number 039 NEBR BRAND COMMITTEE
Agency Division
Fund 23910 BRND INSP & THEFT PR

| | ACCOUNT CODE AND DESCRIPTION | | DEBIT CURRENT MONTH | CREDIT CURRENT MONTH | ACCOUNT BALANCE DEBIT | ACCOUNT BALANCE CREDIT |
|---|---|---|---|---|---|---|
| Expenditures | 570000 | Travel Expenses | | | | |
| | 571100 | LODGING | 2,109.88 | | 12,216.86 | |
| | 571600 | MEALS - TAXABLE | 757.02 | | 2,699.16 | |
| | 571800 | MEALS - TRAVEL STATUS | 371.68 | | 2,519.08 | |
| | 572100 | COMMERCIAL TRANSPORTATIO | | | 276.80 | |
| | 574500 | PERSONAL VEHICLE MILEAGE | 52,463.40 | | 172,658.57 | |
| | 575100 | MISC TRAVEL EXPENSE | 54.00 | | 164.00 | |
| | | Major Account 570000 Total | 55,755.98 | | 190,534.47 | |
| Expenditures | 580000 | Capital Outlay | | | | |
| | 581500 | IMPROVEMENTS TO BUILDINGS | | | 13,659.74 | |
| | 584200 | VEHICLES & VEHICLE EQ | | | 68,206.00 | |
| | | Major Account 580000 Total | | | 81,865.74 | |
| | | Fund 23910 Expenditures Total | 435,788.90 | | 1,846,638.89 | |
| | | Fund 23910 Total | 435,788.90 | 376,806.37 | 1,846,638.89 | 1,610,031.24 |

STATE OF NEBRASKA

Fund Summary By Fund

Menu Version

As of November 30, 2021

Agency Number 039 NEBR BRAND COMMITTEE

Agency Division

Fund 23910 BRND INSP & THEFT PR

| | ACCOUNT CODE AND DESCRIPTION | | DEBIT CURRENT MONTH | CREDIT CURRENT MONTH | ACCOUNT BALANCE DEBIT | ACCOUNT BALANCE CREDIT |
|---|---|---|---|---|---|---|
| Revenues | 470000 | Revenues - Sales & Charges | | | | |
| | 474100 | GENERAL BUSINESS FEES | | 137,731.85 | | 711,659.90 |
| | 474101 | SURCHARGE | | 23,322.35 | | 103,067.10 |
| | 474102 | Auction Markets | | 129,766.10 | | 415,159.10 |
| | 474103 | PACKING HOUSE | | 27,371.70 | | 202,791.70 |
| | 474104 | RFL REGISTERED FED LOTS | | 91,375.00 | | 432,075.00 |
| | 474106 | LATE NOTICE SURCHARGE | | 1,100.00 | | 2,150.00 |
| | 474108 | EXPIRED AND REINSTATED | | 3,460.00 | | 23,480.00 |
| | 474109 | ADD FREEZE | | 75.00 | | 325.00 |
| | 474110 | ADD LOCATION | | 105.00 | | 315.00 |
| | 474111 | Brand Lease | | | | 6.00 |
| | 474112 | BRANDS-NEW | | 4,300.00 | | 22,010.00 |
| | 474113 | BRANDS-RENEWAL | | 35,500.00 | | 119,350.00 |
| | 474114 | BRANDS-TRANSFER | | 1,520.00 | | 9,160.00 |
| | 474115 | BRANDS-DUPLICATE CERTIFIC | | | | 1.00 |
| | 474116 | GRAZING PERMITS | | | | 75.00 |
| | 474118 | OUT-OF-STATE BRANDING PERMIT | | | | 100.00 |
| | | Major Account 470000 Total | | 455,627.00 | | 2,041,724.80 |
| Revenues | 480000 | Revenues - Miscellaneous | | | | |
| | 481100 | INVESTMENT INCOME | | 3,160.59 | | 17,356.42 |
| | 484500 | REIMB NON-GOVT SOURCES | | 2,082.48 | | 13,379.89 |
| | 486600 | CREDIT CARD CLEARING | | 24,152.03 | | 22,583.03 |
| | | Major Account 480000 Total | | 29,395.10 | | 53,319.34 |
| Revenues | 490000 | Other Financing Sources | | | | |
| | 491300 | SALE - SURP PROP/FIXED ASSET | | | | 9.20 |
| | | Major Account 490000 Total | | | | 9.20 |
| | | Fund 23910 Revenues Total | | 485,022.10 | | 2,095,053.34 |
| Expenditures | 510000 | Personal Services | | | | |
| | 511100 | PERMANENT SALARIES-WAGES | 187,477.22 | | 920,500.33 | |
| | 511106 | INTERMITTENT SALARIES | 38,464.83 | | 136,560.25 | |
| | 511700 | EMPLOYEE BONUSES | 990.00 | | 5,790.00 | |
| | 511800 | COMPENSATORY TIME PAID | 713.73 | | 53,895.25 | |
| | 512100 | VACATION LEAVE EXPENSE | 31,793.03 | | 60,475.10 | |
| | 512200 | SICK LEAVE EXPENSE | 17,847.37 | | 36,185.67 | |
| | 512300 | HOLIDAY LEAVE EXPENSE | 9,167.83 | | 47,892.44 | |
| | 512500 | FUNERAL LEAVE EXPENSE | 729.97 | | 1,907.95 | |
| | 512600 | CIVIL LEAVE EXPENSE | 1,348.16 | | 1,348.16 | |
| | 515100 | RETIREMENT PLANS EXPENSE | 18,650.93 | | 84,031.03 | |

Agency Number 039 NEBR BRAND COMMITTEE
Agency Division
Fund 23910 BRND INSP & THEFT PR

| | ACCOUNT CODE AND DESCRIPTION | DEBIT CURRENT MONTH | CREDIT CURRENT MONTH | ACCOUNT BALANCE DEBIT | ACCOUNT BALANCE CREDIT |
|---|---|---|---|---|---|
| Expenditures | 510000 Personal Services | | | | |
| | 515200 FICA EXPENSE | 20,771.77 | | 90,341.90 | |
| | 515500 HEALTH INSURANCE EXPENSE | 51,967.72 | | 255,726.88 | |
| | 516300 EMPLOYEE ASSISTANCE PRO | | | 716.88 | |
| | 516500 WORKERS COMP PREMIUMS | | | 36,023.00 | |
| | Major Account 510000 Total | 379,922.56 | | 1,731,394.84 | |
| Expenditures | 520000 Operating Expenses | | | | |
| | 521100 POSTAGE EXPENSE | 2,005.24 | | 5,510.23 | |
| | 521300 FREIGHT EXPENSE | 226.41 | | 1,057.95 | |
| | 521400 CIO CHARGES | 14,626.85 | | 73,548.89 | |
| | 521500 PUBLICATION & PRINT EXP | 3,348.40 | | 8,943.37 | |
| | 521900 AWARDS EXPENSE | | | 226.55 | |
| | 522100 DUES & SUBSCRIPTION EXP | | | 1,541.42 | |
| | 522200 CONFERENCE REGISTRATION | | | 2,585.00 | |
| | 523201 NATURAL GAS | 195.68 | | 323.43 | |
| | 523202 ELECTRICITY | 215.64 | | 1,561.36 | |
| | 523203 WATER | 43.84 | | 336.49 | |
| | 523204 SEWER | 4.71 | | 23.40 | |
| | 524600 RENT EXPENSE-BUILDINGS | 1,416.99 | | 7,084.95 | |
| | 525100 RENT EXP-OFFICE EQUIP | | | 1,194.00 | |
| | 526100 REP & MAINT-REAL PROPERT | 30.49 | | 12,513.15 | |
| | 527200 REP & MAINT-MOTOR VEHICL | 20.00 | | 3,077.14 | |
| | 531100 OFFICE SUPPLIES EXPENSE | 1,730.67 | | 10,778.93 | |
| | 532200 PERSONAL COMPUTING EQUIPMENT | | | 3,467.27 | |
| | 533132 UNIFORMS | | | 3,515.84 | |
| | 534800 CONST & MAINT SUP EXP | | | 16.75 | |
| | 538182 OIL | 63.92 | | 63.92 | |
| | 538184 FLUIDS | 8.84 | | 8.84 | |
| | 538185 GASOLINE | 4,057.54 | | 8,831.21 | |
| | 541100 ACCTG & AUDITING SERVICES | 29,632.78 | | 117,723.20 | |
| | 541500 LEGAL SERVICES EXPENSE | 1,422.82 | | 5,022.82 | |
| | 541700 LEGAL RELATED EXPENSE | | | 30.00 | |
| | 547100 EDUCATIONAL SERVICES | 360.00 | | 920.00 | |
| | 548500 LAWN/LANDSCAPE/SNOW REMOVAL | | | 368.00 | |
| | 548700 REFUSE/RECYCLING | 45.50 | | 273.00 | |
| | 548900 WEED CONTROL | 275.00 | | 550.00 | |
| | 549200 JANITORIAL/SECURITY SRVS | 58.59 | | 351.54 | |
| | 555200 SOFTWARE - NEW PURCHASES | | | 2,400.00 | |
| | 556100 INSURANCE EXPENSE | 475.75 | | 2,949.75 | |
| | 556300 SURETY & NOTARY BONDS | | | 44.00 | |

As of November 30, 2021

Agency Number 039 NEBR BRAND COMMITTEE
Agency Division
Fund 23910 BRND INSP & THEFT PR

| | ACCOUNT CODE AND DESCRIPTION | DEBIT CURRENT MONTH | CREDIT CURRENT MONTH | ACCOUNT BALANCE DEBIT | ACCOUNT BALANCE CREDIT |
|---|---|---|---|---|---|
| Expenditures | 520000 Operating Expenses | | | | |
| | 559100 OTHER OPERATING EXP | 746.23 | | 6,935.89 | |
| | Major Account 520000 Total | 61,011.89 | | 283,778.29 | |
| Expenditures | 570000 Travel Expenses | | | | |
| | 571100 LODGING | 2,730.52 | | 14,947.38 | |
| | 571600 MEALS - TAXABLE | 529.58 | | 3,228.74 | |
| | 571800 MEALS - TRAVEL STATUS | 1,102.93 | | 3,622.01 | |
| | 572100 COMMERCIAL TRANSPORTATIO | | | 276.80 | |
| | 574500 PERSONAL VEHICLE MILEAGE | 67,837.34 | | 240,495.91 | |
| | 575100 MISC TRAVEL EXPENSE | 53.00 | | 217.00 | |
| | Major Account 570000 Total | 72,253.37 | | 262,787.84 | |
| Expenditures | 580000 Capital Outlay | | | | |
| | 581500 IMPROVEMENTS TO BUILDINGS | | | 13,659.74 | |
| | 584200 VEHICLES & VEHICLE EQ | | | 68,206.00 | |
| | Major Account 580000 Total | | | 81,865.74 | |
| | Fund 23910 Expenditures Total | 513,187.82 | | 2,359,826.71 | |
| | Fund 23910 Total | 513,187.82 | 485,022.10 | 2,359,826.71 | 2,095,053.34 |

# Nebraska Brand Committee

# Information Security Policy

Payment Card Industry Data Security Standard Compliant

IT Security Policy v1.0
Nebraska Brand Committee Rev Date 12-2021

Template provided by Nebraska State Treasury Department

# About This Document

This document contains the Nebraska State agencies policies as they relate to information security. Throughout this document are references to supporting documents which contain more detailed information and guidance on specific standards and procedures. This document is for internal use only and is not to be distributed.

Table 1 - Revision History

| Version | Date | Author | Description of Change |
|---|---|---|---|
| 1.0 | December 1, 2020 | Rebekah Vineyard | Document created |
| | | | Template provided by Nebraska State Treasury Department |
| | | | |
| | | | |
| | | | |
| | | | |

## Contents

# Build and Maintain a Secure Network and Systems

## Section 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are devices that control computer traffic allowed between State of Nebraska's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within the State of Nebraska's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network.  A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls as defined. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment.

### Section 1.1: Establishment and Implementation of Firewall and Router Configuration Standards

- ❖ Nebraska Information Technology Commission's (NITC) 7-201 Network Edge Device Standard for Entities Choosing to Connect to Network Nebraska[1] document details our policies and procedures for implementation and establishment of firewall and router configuration standards and must be followed.
- ❖ The Firewall and Router Configurations must restrict connections between untrusted networks and system components in the Cardholder Data Environment
- ❖ The Firewall and Router Configurations must prohibit direct public access between the Internet and any system component in the Cardholder Data Environment as stated in NITC 7-101 and NITC 8-101, 4.8.1.3.

[1] See *NITC Standards & Guidelines 7-201*

# Section 2: Do Not Use Vendor Supplied Defaults for System Password and other Security Parameters

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

Nebraska State agencies will always change the vendor-supplied defaults for system passwords and other security parameters before systems are installed in the secure network environment (cardholder data network).

## Section 2.1: Change Vendor Supplied Defaults Prior to Installation

- The vendor-supplied defaults must be changed on all system components prior to installation in the cardholder data network. This includes all passwords and simple network management protocol (SNMP) community strings. (Addresses Payment Card Industry (PCI) DSS Requirement 2.1.a, 2.2.d)
- Any unnecessary default accounts must be removed or disabled prior to installation in the cardholder data network. (Addresses PCI DSS Requirement 2.1.b)
- For wireless environments connected to the cardholder data network or transmitting cardholder data:
    - All default settings for wireless equipment must be changed prior to touching cardholder data. (Addresses PCI DSS Requirement 2.1.1.a-e)
    - Encryption keys or passphrases must be changed anytime anyone with knowledge of the keys leaves the company or changes to a position that does not require knowledge of the keys or passphrases. (Addresses PCI DSS Requirement 2.1.1.a)
    - All wireless device firmware configurations must be updated to support strong encryption for both network authentication and data transmission. (Addresses PCI DSS Requirement 2.1.1.d)

## Section 2.2: System Configuration and Hardening Standards

To establish consistency with SANS, ISO, NIST, CIS, or similar security industry standards and address PCI configuration requirements (e.g., password requirements, log settings, File Integrity Monitoring, anti-virus software, etc.), state agencies require documented standards to be developed that address all system components and address all known security vulnerabilities for systems used in the cardholder data network. The NITC Standards & Guidelines 8-103[2] document, details our policies and procedures for configuration and hardening of the system.

- These standards must be updated as new vulnerabilities are identified (See Section 6.1) and be applied when new systems used in the card network are configured and before systems are placed into production.

[2] See the *NITC Standards & Guidelines 8-103* document.

## Section 2.3: Use Secure Protocols for Non-Console Access

- Strong cryptography must be used for any non-console or web-based management interface used for administration of systems or system components.  (Use technologies such as SSH, VPN, or the latest secure versions of TLS (1.1 or higher) for web-based management and other non-console administrative access.) (Addresses PCI DSS Requirement 2.3)

## Section 2.4: System Inventory

- Each state agency maintains an inventory of system components relevant to the scope of PCI DSS. (This should include a system inventory for systems within the Cardholder Data Environment, critical software, any third party payment solutions being used (if applicable), service providers with which cardholder data is being shared (if applicable). See Appendix E.

## Section 2.6: Shared Hosting Providers

- Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A of the PCI Standards Document: Additional PCI DSS Requirements for Shared Hosting Providers.* (Addresses PCI DSS Requirement 2.6)

## Section 3: Protect Stored Cardholder Data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. Credit card data has many sensitive components, including the Primary Account Number (PAN), magnetic stripe authentication data (Track1, Track2), Card Verification Code (CVC), and the Personal Identification Number (PIN), etc.

The following policies address the treatment of credit card data.

### Section 3.2: Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?

- ❖ POS systems are to be updated with the most current version of software that is provided by the manufacturer which does not store the full contents of any track from the magnetic stripe (located on the back of the card, contained in a chip, or elsewhere). Document all software upgrades on the Processing Equipment Maintenance Form.
- ❖ Do not store the card verification code or value (three-digit or four-digit number printed on the bank of the payment card) used to verify card-not-present transactions.
- ❖ Do not store the personal identification number (PIN) or the encrypted PIN block.

### Section 3.3: Mask Credit Card Numbers in Displays Wherever Possible

- ❖ Credit card PAN Data will be masked or truncated when displaying card numbers (Standards say the first six and last four digits are the maximum number of digits to be displayed) on any media. However, we recommend that only the last four digits be printed on any receipt or report. Only personnel with a legitimate business need and proper written approval can see more than the last four digits of the PAN[3]. (Addresses PCI DSS Requirement 3.3)

[3] See Appendix A (*Authorized Users List)*

# Section 4: Encrypt Transmission of Cardholder Data across Open, Public Networks

Cardholder data must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

## Section 4.1: Transmission of Card Data over Public Networks **(If applicable)**

- Strong cryptography and security protocols (e.g., TLS 1.1 or higher, IPSEC, SSH greater than v1.0) must be used whenever cardholder data is transmitted or received over open, public networks. The following controls must be part of the State of Nebraska/NITC data transmission policies: (Addresses PCI DSS Requirement 4.1.a)
    - Only trusted keys and certificates will be accepted. (Addresses PCI DSS Requirement 4.1.b)
    - The data transmission protocol only supports secure versions or configurations and does not support insecure versions or configuration. (e.g., use the latest secure TLS and SSH versions only). (Addresses PCI DSS Requirement 4.1.c)
    - The encryption strength is appropriate for the encryption methodology in use. (Addresses PCI DSS Requirement 4.1.d)
    - For TLS implementations, TLS must be enabled whenever cardholder data is transmitted or received. (Addresses PCI DSS Requirement 4.1.e)
    - If SSL or early TLS is used on a POS POI terminal, a migration plan must be created and implemented, documentation must be created detailing how it was verified that the terminal is not susceptible to any known exploits for SSL or early versions of TLS. Documentation must include evidence (vendor documentation, system/network configuration details, etc). (Addresses PCI DSS Requirement 4.1.f)
    - If SSL or early TLS is used anywhere but a POS POI terminal, a risk mitigation and migration plan must be created, which includes the following: (Addresses PCI DSS Requirement 4.1.g)
        - Description of how it is used, including what data is being transmitted, the types and number of systems that use and/or support SSL or early TLS and the type of environment.
        - The risk assessment results, including the risk reduction controls that are in place.
        - A process of how new vulnerabilities associated with SSL and early TLS are monitored.
        - A description of change control processes that are in place to ensure no new environments are created which utilize SSL and/or early TLS.
        - An overview of the migration project plan that includes a migration completion date no later than June 30th, 2018.

  - If wireless networks transmitting cardholder data or connected to the cardholder data environment are in use, a documented standard must be created which ensures the use of strong encryption and industry best practices. (Addresses PCI DSS Requirement 4.1.1)

## Section 4.2: Transmission of Card Data via End User Messaging Technologies

- It is prohibited to transmit unencrypted cardholder data via end-user messaging technologies (e.g., e-mail, instant messaging, etc.). (Addresses PCI DSS Requirement 4.2)

# Section 5: Protect All Systems against Malware and Regularly Update Anti-Virus Software or Programs

Malicious software, commonly referred to as malware, enters a sensitive network segment during many business approved activities, including employees' e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

## Section 5.1: Deploy anti-virus software to protect systems

- ❖ Anti-virus software must be deployed on all systems in the card network that are commonly affected by malicious software. This includes personal computers, servers, etc. that are attached to the cardholder network segment. (Addresses PCI DSS Requirement 5.1)
- ❖ Anti-virus programs must be capable of detecting, removing, and protecting against all known types of malicious software (adware, spyware, etc.). (Addresses PCI DSS Requirement 5.1.1)
- ❖ For systems considered not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats to confirm whether such systems continue not to require anti-virus software. (Addresses PCI DSS Requirement 5.1.2)

## Section 5.2: Ensure that all anti-virus mechanisms are maintained

- ❖ All anti-virus software and its associated definition files must be kept up-to-date at all times. (Addresses PCI DSS Requirement 5.2.a)
- ❖ All anti-virus software must be actively running, configured to perform automatic updates, and set to run periodic scans. (Addresses PCI DSS Requirement 5.2.b & c)
- ❖ Anti-virus software must be capable of generating audit logs and audit logs must be retained for one year. (Addresses PCI DSS Requirement 5.2.d)

## Section 5.3: Ensure that all anti-virus mechanisms are actively running

- ❖ All anti-virus software installations and configurations must be actively running at all times. (Addresses PCI DSS Requirement 5.3.a)
- ❖ Anti-virus configurations do not allow users to disable or alter the software unless specifically authorized by management on a case-by-case basis for a limited time. (Addresses PCI DSS Requirement 5.3.b & c)

## Section 6: Develop and Maintain Secure Systems and Applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software.

**Note:** Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations.

### Section 6.1: Vulnerability risk ranking process

- ❖ System administrators are to subscribe to outside sources for security vulnerability information and system configuration standards are to be reviewed and updated as new vulnerability information might dictate. Outside sources might include SecurityFocus, A/V companies, SANS, CIS, Secunia, Microsoft, etc. (Addresses PCI DSS Requirement 6.1)

When any vulnerability (or potential vulnerability) is found using NITC Standards & Guidelines 8-101[4], it must be evaluated and assigned a ranking based on the risk level. At a minimum, the highest risk vulnerabilities should be assigned a "High" risk ranking. (Addresses PCI DSS Requirement 6.1)

### Section 6.2: Regularly update systems and software

Patch Management Process

- ❖ All system components and software must have the latest vendor-supplied security patches installed. (Addresses PCI DSS Requirement 6.2.a)
- ❖ All critical system and software patches must be installed within 30 days of vendor release. (Addresses PCI DSS Requirement 6.2.b)
- ❖ A server's OS version, all packages and installed applications versions and patch levels are inventoried centrally. Each system's list of software is compared to a master list of minimum required versions in order to ensure there are no security vulnerabilities present. The master list is maintained by automatically retrieving a list of latest patch levels, as well as by monitoring for security alerts in mailing lists and security web sites for all installed applications.

As industry best practices for vulnerability management are updated, NITC will modify vulnerability management practices to stay in sync with the most recent developments. Procedures related to PCI DSS 6.5.1-6.5.10 will be modified to match industry best practices. (Addresses PCI DSS Requirement 6.5)

[4] See the *NITC Standards & Guidelines 8-101* document.

## Section 6.6: Protect Exposed Web Applications

For public-facing web applications, ensure that either one of the following is in place:

- ❖ Public-facing web applications must be reviewed (using either manual or automated vulnerability security assessment tools or methods) as follows: (Addresses PCI DSS Requirement 6.6)
    - ➢ At least annually.
    - ➢ After any changes.
    - ➢ By an organization that specializes in application security (can be a separate internal company team, independent of the development team that has been trained appropriately).
    - ➢ All vulnerabilities in PCI DSS Requirement 6.5 are included.
    - ➢ All vulnerabilities must be corrected.
    - ➢ The application is re-evaluated after corrections have been made.
- ❖ Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, which continually checks all traffic. The solution must meet the following requirements: (Addresses PCI DSS Requirement 6.6)
    - ➢ Is situated in front of public-facing web applications.
    - ➢ Is actively running and updated as applicable.
    - ➢ Is generating audit logs.
    - ➢ Is configured to either block web-based attacks, or generate an alert.

## Section 7: Restrict Access to Cardholder Data by Business Need to Know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. “Need to know” is when access rights are granted to the least amount of data and privileges needed to perform a job.

### Section 7.1: Limit Access to Cardholder Data and Systems in Cardholder Data Environment

- Access to cardholder data and system components must be restricted to only those individuals whose job requires such access. (Addresses PCI DSS Requirement 7.1)
- Define access needs for each role, including: (Addresses PCI DSS Requirement 7.1.1)
    - System components and data resources that each role needs to access for their job function.
    - Level of privilege required for accessing resources (for example, user, administrator, etc.).
- Restrict access to privileged user IDs to the least privileges necessary to perform job responsibilities and assigned to only those roles that specifically require the privileged access. (Addresses PCI DSS Requirement 7.1.2)
- Access assigned to individual personnel is based on their job classification and function. (Addresses PCI DSS Requirement 7.1.3)
- Require an authorization form specifying all required access privileges, which must be generated and signed by management approving the access. (Addresses PCI DSS Requirement 7.1.4)

### Section 7.2: Access Control Systems

- Access control systems for systems components must restrict access based on a user’s need to know. (Addresses PCI DSS Requirement 7.2)
- Access controls are required on all system components of the cardholder data environment and must be implemented via an automated access control system. (Addresses PCI DSS Requirements 7.2.1)
- Access controls are required to enforce privileges assigned to individuals based on job classification and function. (Addresses PCI DSS Requirements 7.2.2)
- Access control systems must also be set to a default “deny-all” setting. (Addresses PCI DSS Requirements 7.2.3)

## Section 8: Identify and Authenticate Access to System Components

Assigning a unique identification (ID) to each person with access to critical systems or software ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. Note that these requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. This includes accounts used by vendors and other third parties (for example, for support or maintenance). These requirements do not apply to accounts used by consumers (e.g., cardholders).

### Section 8.1: Require Unique User IDs

- Unique IDs will be used for all users that access system components or cardholder data. (Addresses PCI DSS Requirement 8.1.1)
- Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. (Addresses PCI DSS Requirement 8.1.2)
- Immediately revoke access for any terminated users. (Addresses PCI DSS Requirement 8.1.3)
- Remove/disable inactive user accounts at least every 90 days. (Addresses PCI DSS Requirement 8.1.4)
- Manage IDs used by all third parties with remote access to access, support, or maintain system components via remote access, ensuring that they are only enabled for the time period needed, disabled when not in use, and they are monitored by agency employees during use. (Addresses PCI DSS Requirement 8.1.5)
- Limit repeated access attempts by locking out the user ID after not more than six attempts. (Addresses PCI DSS Requirement 8.1.6)
- Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. (Addresses PCI DSS Requirement 8.1.7)
- If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. (Addresses PCI DSS Requirement 8.1.8)

### Section 8.2: User Authentication Methods

- In addition to assigning a unique user ID, access to systems in the card network requires the use of at least one of the following: (Addresses PCI DSS Requirement 8.2)
  - Something you know, such as a password or passphrase
  - Something you have, such as a token device or smart card
  - Something you are, such as a biometric
- Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. (Addresses PCI DSS Requirement 8.2.1)
- Verify user identity before modifying any authentication credential (for example, performing password resets, provisioning new tokens, or generating new keys.) (Addresses PCI DSS Requirement 8.2.2)
- Passwords or phrases must meet the following: (Addresses PCI DSS Requirement 8.2.3)
  - Require a minimum length of at least seven characters
  - Contain both numeric and alphabetic characters

- ❖ Change user passwords/passphrases at least every 90 days. (Addresses PCI DSS Requirement 8.2.4)
- ❖ Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/phrases they have used. (Addresses PCI DSS Requirement 8.2.5)
- ❖ Set all first time use and reset passwords to a unique value for each user and require immediate change after first use. (Addresses PCI DSS Requirement 8.2.6)

## Section 8.3: Multi-factor Authentication

- ❖ Incorporate multi-factor authentication for remote network access originating from outside the network by personnel, including users and administrators and all third parties, including vendor access for support or maintenance. (Addresses PCI DSS Requirement 8.3)
- ❖ Incorporate multi-factor authentication for all console and non-console access into the CDE for personnel with administrative access. (Addresses PCI DSS Requirement 8.3.1)

## Section 8.4: Password Policy

- ❖ Document and communicate authentication procedures and policies to all users including: (Addresses PCI DSS Requirement 8.4)
    - ➢ Guidelines for selecting strong authentication credentials.
        - ▪ All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed at least every 90 days.
        - ▪ All production system-level passwords must be part of the agency administered password log.
        - ▪ All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.
        - ▪ Passwords must change upon initial logon, system permitting, by the user and subsequently changed at least every 90 days.
        - ▪ All user-level and system-level passwords must conform to the guidelines described below.
    - ➢ Guidelines
        - ▪ All users at a state agency should be aware of how to select strong passwords. Strong passwords have the following characteristics:
            - Contain at least three of the five following character classes:
                - o Lower case characters
                - o Upper case characters
                - o Numbers
                - o Punctuation
                - o “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)
                - o Contain at least ten alphanumeric characters.
            - Weak passwords have the following characteristics:
                - o The password contains less than ten characters
                - o The password is a word found in a dictionary (English or foreign)
                - o The password is a common usage word such as:

        - Names of family, pets, friends, co-workers, fantasy characters, etc.
        - Computer terms and names, commands, sites, companies, hardware, software.
        - The words “State of Nebraska”, "sanjose", "sanfran" or any derivation.
        - Birthdays and other personal information such as addresses and phone numbers.
        - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
        - Any of the above spelled backwards.
        - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
  - Password Protection Standards
    - Always use different passwords for agency accounts from other non-agency access (e.g., personal ISP account, option trading, benefits, etc.).
    - Always use different passwords for various agency access needs whenever possible.
    - Passwords must not repeat any of the four most recently used passwords.
    - Do not share agency passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential agency information.
    - Passwords should never be written down or stored on-line without encryption.
    - Do not reveal a password in email, chat, or other electronic communication.
    - Do not speak about a password in front of others.
    - Do not hint at the format of a password (e.g., "my family name")
    - Do not reveal a password on questionnaires or security forms
    - If someone demands a password, refer them to this document and direct them to the IT Administrator. If an account or password compromise is suspected, report the incident to the IT Administrator
  - Instructions to change passwords if there is any suspicion the password could be compromised.
    - Validating requests to change passwords should include face-to-face verification, or having the team member validate their identity by answering their authentication questions and answers (minimum six questions and three correct answers). Once the team member is positively identified, a new password will be automatically generated (using a valid password generation program) to provide to the team member.

## Section 8.5: Group or Shared Passwords

- Do not use group, shared, or generic password or other authentication methods as follows: (Addresses PCI DSS Requirement 8.5.)
  - Generic user IDs are disabled or removed.
  - Shared user IDs do not exist for system administration and other critical functions.
  - Shared and generic user IDs are not used to administer any system components.

## Section 8.6: Other Authentication Mechanisms

- Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: (Addresses PCI DSS Requirement 8.6)
    - Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts.
    - Physical or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.

## Section 9: Restrict Physical Access to Cardholder Data

Any physical access to data or systems that house cardholder data provide the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, “onsite personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity’s premises. A “visitor” refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. “Media” refers to all paper and electronic media containing cardholder data.

- NITC Standards & Guidelines 8-101[5] document details our policies and procedures for restricting physical access to cardholder data and must be followed at all times. (Addresses PCI DSS Requirements 9.1 – 9.10)
- PCI paper shall not be generated.

### Section 9.5: Are all media physically secured (Including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)?

- All media shall remain within the locked, secured, office premises, until such time, as required for the media, that it is destroyed. If any paper media is created by the card swipe machines, this media will be shredded.

### Section 9.6: Is strict control maintained over the internal or external distribution of any kind of media?

- Locate all paper documents (including receipts, notes, reports and faxes) and all electronic storage data (if any type) which contain your customers’ full credit/debit card numbers and mark the container as “Confidential”.
- Media will not be transported or delivered outside the secured perimeter of the office.
- Only authorized individuals will handle media within the confines of the office secured space.

### Section 9.7: Is strict control maintained over the storage and accessibility of media?

- No material will be removed from the secure area.

### Section 9.8: Is all media destroyed when it is no longer needed for business or legal reasons?

- All hardcopy (paper) media will be destroyed by a crosscut shredder immediately.

### Section 9.9: Are devices that capture payment card data via direct physical interaction with the card protected against tampering and substitution as follows?

- A list of POS devices shall be maintained along with a list of authorized users. This list will include the make and model of device, the location of the device, and the device serial number. The list will be updated when devices are added, relocated, or decommissioned.

[5] See the *NBC Standards & Guidelines 8-101* document.

- Devices will be periodically inspected to look for tampering or substitution by checking the serial number and other device characteristics.  Personnel will be trained annually on how to inspect POS devices for tampering.
- Personnel will be trained to be aware of suspicious behavior and to report tampering or substitution of devices.  Personnel are to verify the identity of repair or maintenance personnel.  Devices will not be installed, replaces, or returned without verification.  Personnel will report any indication of suspicious behavior or of device tampering to their manager.

## Section 10: Track and Monitor All Access to Network Resources and Cardholder Data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

### Section 10.1: Enable Audit Trails to Link Access to System Components

- Enable audit trails on all system components within the cardholder data network to link all access to system components to each individual user. (e.g., server event logs, web server logs, firewall logs, payment application logs, etc.). (Addresses PCI DSS Requirement 10.1)

### Section 10.2: Generation of Automated Audit Trails

- Implement automated audit trails for all system components to capture the following events: (Addresses PCI DSS Requirement 10.2)
    - All individual access to cardholder data.
    - All actions taken by any individual with root or administrative privileges.
    - All access to audit trails.
    - Invalid logical access attempts.
    - Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.
    - Initialization, stopping, or pausing the audit logs.
    - Creation and deletion of system level objects.

### Section 10.3: Audit Trail Entries

- Record at least the following audit trail entries for all system components for each event: (Addresses PCI DSS Requirement 10.3)
    - User Identification
    - Type of event
    - Date and Time
    - Origination of event
    - Identity or name of affected data, system component, or resource

## Section 10.4: Network and System Time Sync

- The Nebraska State Treasurer's Office Network Time Protocol (NTP) Configuration Procedures[6] document details the process for obtaining and distributing a time signal (system time) to all system components within the cardholder data network. (Addresses PCI DSS Requirement 10.4)
- Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time: (Addresses PCI DSS Requirement 10.4)
    - A central timeserver is designated, and if there are multiple servers, the servers are configured to peer with each other to keep accurate time. (Addresses PCI DSS Requirement 10.4.1)
    - All other components in the CDE receive time only from the designated central timeserver. (Addresses PCI DSS Requirement 10.4.1)
    - Critical systems have the correct and consistent time. (Addresses PCI DSS Requirement 10.4.1)
    - Time data is protected through access to time data restricted to only personnel with a business need. (Addresses PCI DSS Requirement 10.4.2)
    - All time settings on critical systems are logged, monitored, and reviewed. (Addresses PCI DSS Requirement 10.4.2)
    - Time settings are received from industry-accepted sources. (Addresses PCI DSS Requirement 10.4.3)

## Section 10.5: Audit Trail Security

- Secure audit trails so they cannot be altered as follows: (Addresses PCI DSS Requirement 10.5)
    - Limit viewing of audit trails to those with a job-related need. (Addresses PCI DSS Requirement 10.5.1)
    - Protect audit trail files from unauthorized modifications. (Addresses PCI DSS Requirement 10.5.2)
    - Promptly back up audit trail files to a centralized log server or media that is difficult to alter. (Addresses PCI DSS Requirement 10.5.3)
    - Write logs for external-facing technologies onto a secure, centralized log server or media device. (Addresses PCI DSS Requirement 10.5.4)
    - Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts. (Addresses PCI DSS Requirement 10.5.5)

## Section 10.6: Log Review

- Review logs and security events for all system components to identify anomalies or suspicious activity. (Addresses PCI DSS Requirement 10.6)
- Review the following at least daily:
    - All security events.
    - Logs of all system components that store, process, or transmit cardholder data, or that could affect the security of cardholder data.
    - Logs of all critical system components.

[6] See the *NBC's Configuration Procedures* document.

    - Logs of all servers and system components that perform security functions (for example, firewalls, IDS/IPS, authentication servers, e-commerce redirection servers, etc.).
- Review logs of all other system components periodically, based on the organization's policies and risk management strategy, as determined by NITC's Annual Risk Assessment[7]. Until NITC Annual Risk Assessment document is complete, the Agency Information Security Officer or designated employee shall review logs from servers and card applications. (Addresses PCI DSS Requirement 10.6.2)
- Immediately follow up on exceptions and anomalies identified during the review process. (Addresses PCI DSS Requirement 10.6.3)

## Section 10.7: Audit Trail History

- Retain audit trail history for at least one year with a minimum of three months immediately available for analysis (e.g., online, archived, or restorable from backup). (Addresses PCI DSS Requirement 10.7)

[7] See the *NBC's Annual Risk Assessment is being addressed*.

## Section 11: Regularly Test Security Systems and Processes

System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment. Detailed testing procedures[8] should be developed and documented to meet the following policies.

### Section 11.1: Rogue Wireless Network Detection

- NITC Standards and Guidelines 7-301[9] describes the documented process that will be used at least quarterly to detect unauthorized wireless networks/devices within the card-processing environment. (Addresses PCI DSS Requirement 11.1 and 11.1.2)
- The defined methodology will address the detection and identification of multiple types of wireless devices such as WLAN cards inserted into system components, portable wireless devices connected to system components, and wireless devices connected to a network port or network device. (Addresses PCI DSS Requirement 11.1)
- Any automated monitoring solution must generate alerts if rogue devices are detected.
- Process documentation must define a response procedure if rogue devices are found.
- Each agency will maintain an inventory of all authorized wireless access points including a documented business justification. (Addresses PCI DSS Requirement 11.1.1)
- The agency will define incident response procedures (see PCI DSS Requirement 12.10) in the event an unauthorized wireless access point is detected (Addresses PCI DSS Requirement 11.1.2)

### Section 11.2: Vulnerability Scans

- Internal vulnerability scans must: (Addresses PCI DSS Requirement 11.2.1.a-c)
    - Be performed by a qualified internal resource with organizational independence or a qualified third party.
    - Have a process to include a rescan until all “high risk” vulnerabilities must be addressed in accordance with the entity’s vulnerability ranking (as defined in Requirement 6.1) and verified by rescans.
- External vulnerability scans must (Addresses PCI DSS Requirement 11.2.2.a-c)
    - Contain no vulnerabilities that are scored 4.0 or higher by the CVSS.
    - Run on all external IP addresses that could be used to gain access to the cardholder data environment. (Addresses PCI DSS Requirement 11.2)

- The agency must ensure that results of each quarter's internal and external vulnerability assessments are to be documented and retained for review. (Addresses PCI DSS Requirement 11.2.3) State OCIO can assist upon request.

## Section 11.3: Penetration Testing

- Implement a methodology for penetration testing that includes the following: (Addresses PCI DSS Requirement 11.3)
    - Is based on industry-accepted penetration testing approaches. (for example, NIST SP 800-115)
    - Includes coverage for the entire CDE perimeter and critical systems.
    - Includes testing from both inside and outside the network.
    - Includes testing to validate all segmentation and scope reducing controls.
    - Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5.
    - Defines network-layer penetration tests to include components that support network functions as well as operating systems.
    - Includes review and consideration of threats and vulnerabilities experienced in the last 12 months.
    - Specifies retention of penetration testing results and remediation activity results for at least one year.
- Internal and external penetration tests are to be performed as per the defined methodology, at least annually and after any significant infrastructure or application upgrade or modification (e.g., an operating system upgrade, a sub-network added to the environment, or a web server added to the environment, etc.). (Addresses PCI DSS Requirement 11.3.1 and 11.3.2)
- Penetration testing is to be performed by a qualified internal resource or third party. If an internal resource is used, the personnel conducting the test must be independent from personnel that work within the cardholder environment. (PCI DSS Requirement 11.3)
- Exploitable vulnerabilities found during testing are corrected and testing is repeated to confirm the correction. (Addresses PCI DSS Requirement 11.3.3)
- If segmentation is used to isolate the CDE from other networks, perform penetration tests (performed by a qualified internal resource or qualified external third party) at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems. (Addresses PCI DSS Requirement 11.3.4)
- If the entity is a service provider: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods. This requirement is a best practice until January 31, 2018, after which it becomes a requirement. (Addresses PCI DSS Requirement 11.3.4.1)

## Section 11.4: Intrusion Detection/Prevention

- All traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder environment must be monitored by the use of an Intrusion Detection System (IDS) and/or Intrusion Prevention System (IPS). (Addresses PCI DSS Requirement 11.4.a)

- The IDS/IPS system(s) must be configured to alert personnel of suspected compromises. (Addresses PCI DSS Requirement 11.4.b)
- All IDS/IPS system(s) must be kept up to date with the latest available attack signatures. (Addresses PCI DSS Requirement 11.4.c)

## Section 11.5: Change Detection

- Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. (Addresses PCI DSS Requirement 11.5)

## Section 12: Maintain a Security Policy that Addresses Information Security for All Personnel

A strong security policy sets the security tone for the State of Nebraska and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. "Employees" refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the State of Nebraska's site.

### Section 12.1: Publish, Distribute, and Update the Information Security Policy

- The Nebraska Brand Committee requires that the most recent version of the information security policy be published and disseminated to all relevant system users (including vendors, contractors, and business partners). (Addresses PCI DSS Requirement 12.1)
- The Nebraska Brand Committee information security policy must be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. (Addresses PCI DSS Requirement 12.1.1)

### Section 12.2: Implement a Risk-Assessment Process

- NITC defines and documents a risk assessment process in the NITC Standards & Guidelines[10] document, which: (Addresses PCI DSS Requirement 12.2)
  - Is performed annually and upon significant change to the environment
  - Identifies critical assets, threats, and vulnerabilities
  - Results in a formal risk assessment.

### Section 12.3: Critical Technology Usage Policies

- The State of Nebraska must develop usage policies for critical technologies (e.g., remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage), and define proper use of these technologies. (Addresses PCI DSS Requirement 12.3)
- Explicit management approval is required prior to using the technologies. (Addresses PCI DSS Requirement 12.3.1)
- Any use of the technology must be authenticated with a user ID and password or other authentication item (for example, token). (Addresses PCI DSS Requirement 12.3.2)
- A list must be maintained of all such devices in use and contain the personnel authorized to use them in the State of Nebraska agency Critical Technology Device Inventory Document Attachment F. (Addresses PCI DSS Requirement 12.3.3)
- A method to determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices) accurately and readily. (Addresses PCI DSS Requirement 12.3.4)
- Acceptable uses for the technology must be defined and documented (This should include a system inventory for systems within the Cardholder Data Environment, critical software, any third party payment

[10] See the *NITC Standards & Guidelines Risk Assessment Process* document.

solutions being used (if applicable), service providers with which cardholder data is being shared (if applicable). (Addresses PCI DSS Requirement 12.3.5)

- ❖ Acceptable network locations for the technologies must be defined and documented. (Addresses PCI DSS Requirement 12.3.6)
- ❖ A list of company-approved products must be kept. (Addresses PCI DSS Requirement 12.3.7)
- ❖ Remote-access technologies in use must automatically disconnect sessions after a specific period of inactivity. (Addresses PCI DSS Requirement 12.3.8)
- ❖ Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners with immediate deactivation after use. (Addresses PCI DSS Requirement 12.3.9)
- ❖ Copying, moving, or storing cardholder data on local hard drives and removable electronic media when accessing such data via remote-access technologies is prohibited unless explicitly authorized for a defined business need, and the cardholder data is protected in accordance with all applicable PCI DSS requirements. (Addresses PCI DSS Requirement 12.3.10)

## Section 12.4: Assign Information Security Responsibilities and Train Employees

- ❖ Nebraska Brand Committee Information Security Policy and procedures clearly define information security responsibilities for all personnel (Addresses PCI DSS Requirement 12.4)
  - ➢ If the agency is a service provider: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include overall accountability for maintaining PCI DSS compliance and defining a charter for a PCI DSS compliance program and communication to executive management. (Addresses PCI DSS Requirement 12.4.1)

## Section 12.5: Assign Information Security Management

- ❖ **The overall responsibility of information security management falls under the Agency Information Security Officer or designated agency personnel.** (Addresses PCI DSS Requirement 12.5)

- ❖ The following responsibilities must be assigned: (see the Management Roles and Responsibilities form in Appendix B)
  - ➢ Establishing, documenting, and distributing the Nebraska Brand Committee's information security policies and procedures. (Addresses PCI DSS Requirement 12.5.1)
  - ➢ Responsibility to monitor, analyze, and distribute security alerts and information. (Addresses PCI DSS Requirement 12.5.2)
  - ➢ Establishing detailed documentation of security incident response and escalation procedures and formally assign the responsibility of creating and distributing these procedures to a specific role, position, or team. (Addresses PCI DSS Requirement 12.5.3)
  - ➢ Administration of user accounts in the cardholder data network. (Addresses PCI DSS Requirement 12.5.4)
  - ➢ Monitoring and controlling all access to data. (Addresses PCI DSS Requirement 12.5.5)

## Section 12.6: Security Awareness Program

- NTIC Standards & Guidelines 8-101 document[11] defines the processes used by the agency to ensure personnel are aware of the cardholder data security policy and procedures. (Addresses PCI DSS Requirement 12.6.a)
- Employees working in the cardholder data environment must be educated upon hire and at least annually regarding their data security responsibilities. (Addresses PCI DSS Requirement 12.6.b)
- Security awareness training programs must employ the use of multiple methods of communicating awareness and educating employees (e.g., posters, letters, memos, web-based training, meetings, promotions, etc.). (Addresses PCI DSS Requirement 12.6.1.a)
- Employees must acknowledge in writing, at least annually, that they have read and understood the Nebraska Brand Committee Security Policies and Procedures. (Addresses PCI DSS Requirement 12.6.2)

## Section 12.7: Background Checks

- Background checks are to be conducted, within the constraints of local laws, on employees, prior to hire, who will have access to cardholder data or the cardholder data environment. (Addresses PCI DSS Requirement 12.7) State of Nebraska agencies should at least do driver records, county and district court records, and a State Patrol check.

## Section 12.8: Policies for Sharing Data with Service Providers

- In order to conform to industry best practices, it is required that due diligence be performed before engaging with new service providers and is monitored for current service providers that store, process, or transmit cardholder data on behalf of the state agency. Service providers, which could affect the security of sensitive cardholder data, are also in-scope of this policy. The Nebraska State Treasurer's Office Full-Service Provider Compliance Validation Procedures[12] document describes the process of validating service provider compliance with PCI DSS Requirements. (Addresses PCI DSS Requirement 12.8)

## Section 12.9: Additional Requirements for Service Providers

- Service providers must acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. (Addresses PCI DSS Requirement 12.9)

## Section 12.10: Incident Response Plan Policies

- The Nebraska State Treasurer's Office Incident Response Plan[13] document (IRP) explains the course of action in the event of a breach or suspected breach.
- IRP will be reviewed and tested at least annually.

[11] See the *NITC Standards & Guidelines 8-101* document.

[12] See the *Nebraska State Treasurer's Office Full-Service Provider Compliance Validation Process* document.

[13] See the *Nebraska State Treasurer's Office Incident Response Plan*

- A Computer Incident Response Team (CIRT) will consist of members from the State Agency, OCIO and State Treasurer's Office.
- Team members designated are to be available on a 24/7 basis to respond to alerts.
- Team members are required to understand data breach response requirements outline by each card brand.
- Training will be provided to staff with security breach response responsibilities.
- Each Team will have the following members identified and reviewed at least annually.

| CIRT Members | CIRT Role |
|---|---|
| Agency Director/Manager | Provide authority to operate and has authority to make business-related decisions based on information garnered from the other team members. |
| State Information Security Officer | Assess security incidents, perform containment, eradication and basic forensics. Assist information technology in recovery role. |
| Agency Information Security Officer | Minimize the impact to system end users. Assist the Information Security team with technical issues and recovery roles. |
| Chief Information Officer | Understand the root cause of the incident and any failures of compliance, which may have contributed to the incident. |
| Network Services Administrator | Assess any physical damage and investigate any physical theft of data. Document chain of custody for any physical evidence. |
| Agency Legal | Ensure that evidence collected is usable in a criminal investigation. Act as legal counsel to senior management. |
| Agency Human Relations Representative | Provide advice to senior management if an employee caused the incident. |
| Public Relations – State Treasurer's Office Staff | Work with all members of the CIRT to understand the incident. Coordinate with senior management, acquirers, card brands and law enforcement to develop a disclosure plan (if any). |

## Appendix A – Authorized Users List

# Authorized Users List

Below is a list of users authorized to view full PAN data as required by PCI DSS Requirement 3.3 and approved by the director of the agency.

[Employee Full Name]

[Employee Full Name]

[Employee Full Name]

[Employee Full Name]

# Appendix B – Management Roles and Responsibilities

## Assignment of Management Roles and Responsibilities for Security

As required by policy in Section 12.5 of this security policy, the following table contains the assignment of management roles for security processes.

Table A1 - Management Security Responsibilities

| Name of Role, Group, or Department | Date Assigned | Description of Responsibility |
|---|---|---|
| | | Establish, document, and distribute security policies |
| | | Monitor, analyze, and distribute security alerts and information |
| | | Establish, document, and distribute security incident response and escalation policies |
| | | Administration of user accounts on systems in the cardholder data network |
| | | Monitor and control all access to cardholder data |

# Appendix C – Agreement to Comply with Information Security Policies

## Agreement to Comply with Information Security Policies

All employees working with cardholder data must submit a signed paper copy of this form. Agency management will not accept modifications to the terms and conditions of this agreement.

I, the user, agree to take all reasonable precautions to assure that agency's internal information, or information that has been entrusted to the agency by third parties, such as customers, will not be disclosed to unauthorized persons. At the end of my employment or contract with the agency, I agree to return all information to which I have had access as a result of my position with the agency. I understand that I am not authorized to use this information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal agency manager who is the designated information owner.

I have access to a copy of the Nebraska State Treasurer's Office Information Security Policies Manual, I have read and understand the manual, and I understand how it affects my job. As a condition of continued employment at the State agency, I agree to abide by the policies and other requirements found in that manual. I understand that non-compliance will be cause for disciplinary action up to and including system privilege revocation, dismissal from the agency, and perhaps criminal and/or civil penalties.

I agree to choose a difficult-to-guess password as described in the Nebraska State Treasurer's Office Information Security Policies Manual, I agree not to share this password with any other person, and I agree not to write this password down unless it has been transformed in an unrecognizable way.

I also agree to promptly report all violations or suspected violations of information security policies to the agency director and/or OCIO's office.

List what program(s) the employee has access to and why the business need for credit card information.

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

_________________________________________ _________________________________________
Employee's Printed Name Employee's Title

Template provided by Nebraska State Treasury Department

____________________________________________

Employee’s Telephone Number

____________________________________________

Employee’s Physical Address

____________________________________________

Employee’s Signature

____________________________________________

Agency Director Signature

# Appendix D – Wireless Access Point Inventory

## Wireless Access Point Inventory

All agencies must maintain an inventory of all wireless access points.

| Make & Model | Manufacturer | Serial Number | Mac Address | Managed By | Business Reason |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

## Appendix E – System Inventory

### Inventory Spreadsheet

| Device Vendor | Device Model Name(s) and Number | Device Location | Device Status | Serial Number or Other Unique Identifier |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## Appendix F – Critical Technology Device Inventory

### Critical Technology Device Inventory Spreadsheet

Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, email usage and internet usage.  Define proper use of these technologies and the personnel approved to access.

| Type | Manufacturer | Product Name | Purpose | Users with Access | Usage Approved By |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

# NEBRASKA BRAND COMMITTEE

411 Niobrara Ave. Alliance, NE USA 69301-0775
308-763-2930 • www.nbc.nebraska.gov

**INSPECT • RECORD • POLICE**

Help us recruit great talent to our team!

We are constantly working to attract and recruit top talent to join our team. One area of particular focus due to critical staffing needs has been the recruitment of high-quality candidates to join our team at the Nebraska Brand Committee.

The agency is implementing a $250.00 referral bonus to assist in staffing any open positions. The referral bonus is available to any current teammate who refers newly hired brand inspectors who successfully complete their probation period. This program is designed to help recruit new great teammates like you to our team.

Specifics about the referral program, as well as tools to help in your recruiting efforts, can be found in the below:

- A $250.00 referral bonus is available to any current teammate who refers a newly hired teammate for any open position within the agency.
- The bonus is available to teammates who were employed by the Nebraska Brand Committee, as a permanent teammate as of September 27, 2021 and/or before September 27, 2022.
- The referring teammate's name must be listed on the application to receive the bonus payment.
- The bonus will be paid to the qualifying teammate for each referred new hire who completes original probation. The payment will be made in the pay period following the successful original probation end date of the referred new hire. Note, teammate must be employed by the State of Nebraska at the end of a pay period for which the payment is scheduled to be made.
- New hires may include former state teammates who are eligible for rehire as a permanent teammate.
- There is no limit to the number of people who may be referred.

NEBRASKA BRAND COMMITTEE

Post Office Box I • 411 Niobrara Ave.
Alliance, NE USA 69301-0775

INSPECT • RECORD • POLICE

# NEBRASKA BRAND COMMITTEE
# PERSONNEL CHANGES- September 1, 2021-November 30, 2021

## FULL TIME EMPLOYEES

| | | |
|---|---|---|
| 9/1/2021 | Darcy Stewart Ramos | Kearney |
| 9/1/2021 | Richard Estergard | In Charge-Broken Bow |
| 10/1/2021 | Sam Day | Full time to Intermittent |
| 10/1/2021 | Sarah McCown | Kearney |
| 10/1/2021 | Bryce Davis | Inspector In-Charge Ogallala |
| 10/1/2021 | Shawn Lake | Intermittent to Full Time Floater Position |
| 10/1/2021 | Zane Snyder | Intermittent to Full Time |
| 10/15/2021 | John Robert Fadden | Resigned-Banner County |
| 10/18/2021 | Josh Cox | Kearney Full Time |
| 10/22/2021 | Cody Waite | Resigned- West Supervisor |
| 10/31/2021 | Sam Day | Resigned- Valentine |
| 11/1/2021 | Tryssta Duvel | Kearney Full Time |
| 11/29/2021 | Jeremy Kennedy | Intermittent to Full Time Crawford |
| | | |

## INTERMITTENT INSPECTORS

| | | |
|---|---|---|
| 10/1/2021 | Zane Snyder | Moved to Full Time |
| 10/1/2021 | Shawn lake | Moved to Full Time |
| 10/1/2021 | Kevin Meyer | Intermittent Valentine |
| 11/29/2021 | Jeremy Kennedy | Moved to Full Time |

## OPEN POSITIONS

| | | |
|---|---|---|
| Ogallala | | Full Time |
| Ogallala | | Full Time |
| Osh Kosh | | Full Time |

# NEBRASKA BRAND COMMITTEE

# STRATEGIC PLAN

## INTRODUCTION

The purpose of the Nebraska Brand Committee is to provide individual herd identification through brand recording; ownership protection through brand inspection at markets, during private treaty sales, and when leaving the state and / or brand inspection area; and investigation of cases which involve fraud in marketing of cattle and theft of livestock.

## MISSION

*To be the leader in animal ownership and movement verification for livestock producers.*

## VISION

*By cultivating people, leadership and new technology the Nebraska Brand Committee will be the leader in inspection, recording and policing for the livestock industry.*

Nebraska Brand Committee will pursue our vision by:

- Implementation and completion of electronic reporting system.
- Executing new methodologies for brand inspection to include Electronic Identification.
- Providing continuing education for stakeholders with enhanced communication.
- Enhancing the positive culture within the agency.
- Creating additional value and services to all segments of our producers.
- Cultivating our relationship with other agencies and industry partners.

## PAST: WHERE WE HAVE BEEN

The 1941 Legislature created the Nebraska Brand Committee, it is a totally self-supported cash fund agency, and its mission is accomplished under the authority of Nebraska Livestock Brand Act.

The Nebraska Brand Committee is a non-code agency administrated by 5 Committee Members that are appointed by the governor, employees are divided between administrative personnel, investigators and field personnel.

## PRESENT: WHERE WE ARE NOW

The Nebraska Brand Committee is creating efficiencies with technology by implementing the electronic brand reporting system, electronic brand book, client portal, electronic fee collection and processing. Also implementing other labor saving tasks and eliminating repetitive functions required by a paper based system.

## FUTURE: WHERE WE WANT TO BE

The desire of the Nebraska Brand Committee is to move into the future beside and serving the Livestock Industry, using the most current technologies available. Exploring new ideas and methodologies for brand inspection that would include the ability to utilize electronic animal identifiers.

## THE GOALS SET BY THE NEBRASKA BRAND COMMITTEE TO ACCOMPLISH OUR VISION

1. Continue to develop and build our electronic reporting system.
2. Analyze, monitor and manage agency income and expenditures.
3. Implement a system that allows the Nebraska Brand Committee to utilize Electronic Identifiers as evidence of ownership.
4. Reduce costs of per head inspections.
5. Creating educational strategies for specific stakeholder groups.

## NEBRASKA BRAND COMMITTEE WILL MEASURE SUCCESS WITH KEY PERFORMANCE INDICATORS OF:

□ Retention of employees at 95% annually.
□ Completion of remaining milestones in set project plan.
□ Rollout and training of electronic time keeping program by 3rd quarter 2019-2020.
□ Provide onsite training and demonstration opportunity for legislative leaders.
□ Create close working relationships with the Department of Agriculture for Nebraska Traceability Group.
□ To see a reduction of at least 2.5% per month in mileage reimbursement until it hits the target of a 15% overall annual reduction.
□ To realize a decrease of 2% per month reduction in comp-time pay out and accrual until the target of a 22.5% reduction per annum is reached.
□ Finalization of Best Evidence and Enrollment Requirements to implement Electronic Animal Identifier (EID) brand inspection system.
□ Initial Implementation of Electronic Animal Identifier repository.
□ Implementation of non-change of ownership E-Inspections.
□ Implementation of change of ownership E-Inspection.
□ Development and implementation of Electronic Animal Identifier (EID) Tracking and Information Exchange with Nebraska Department of Agriculture and USDA.
□ Development and implementation of interface to banking systems for lien lookups and collateralization of cattle.
□ Initiate the value add components for producer opt in section on marketing opportunities.
□ Completion of EID E-Inspection, Financial Transactions and Lien perfection and collateralization of cattle.

# Fee Schedule

## Brand Recording Fees

**New Brand Application** - $100.00 (Left & Right sides require two separate applications with separate checks of $100.00 each)

- Add location - $15.00 per location (same side only)
- Add freeze - $25.00 per side

**Brand Transfer** - $40.00

**Brand Renewal** - $50.00 (Every four years)

**Brand Lease** - $1.00 (Only good until renewal date)

**Brand Ownership Certificate** - $1.00 per copy

**Brand Research** - $20.00 per hour & $1.00 per copy

**Brand Inspection Fees**

**Inspection Fee** - $.85 per head (Effective Oct 1, 2021)

**Surcharge** - $20.00 per stop (Effective July 1, 2020)

**48 Hour Late Fee -** $50.00 per inspection (Effective Sept 1, 2021)

**Local Inspection Duplicate** - $6.00 research + $1.00 per copy

**Sale Ring Clearance Duplicate** - $6.00 research + $1.00 per copy

**Local Inspection Research** - $20.00 per hour + $1.00 per copy

**Grazing Permits** - $15.00 per year (Renewed every year)

## Registered Feedlots

**Registered Feedlot Permit** - $1000.00 for each 1,000 head plus $250.00 for each increment of 250 head above the 1,000 head total of the one-time capacity of lot(s) to be registered.

## Out of State Branding Permits - $50.00

The requested brand will have to be verified before any permit is issued by a brand inspector.

*Revised October 1, 2021*

# Technology Report – December 2021

# Danna Schwenk

**Staff Technology Updates**

- Working at Ogallala Sale barn most sale days since Sept 1st on Wednesdays, Thursday and some Mondays. There will be 3 to 4 sales each week for the month of December, so I foresee assisting through at least December and January.
- High Speed internet installed at Broken Bow in November eliminated most issues with Admin.
- Requested OCIO bids on high-speed internet at Bassett, Burwell and Ogallala barns which have continued to have issues with MiFI hotspots. Installation estimated before end of the year.
- Next barns to be bid will be Lexington and Huss in Kearney after discussion with ownership.

**Nebraska Interactive**

- Ongoing update releases are focused on bug fixes and minor updates to improve payment processing issues.
- Planning and sprint meetings ongoing.
- Continued testing of client portal with next update to include company enrollment for portal before first phase will be released hopefully at the beginning of January.
- Announced Sept 15th as a winner of the National Government Experience Project award.
- Was advised by NIC that due to required data framework end of life issues they will be focused on updating all various agency programs to handle these changes. This affects us that only designated legislative required development will be addressed in the next foreseeable year. Bug fixes will still be resolved.

**E-Inspection**

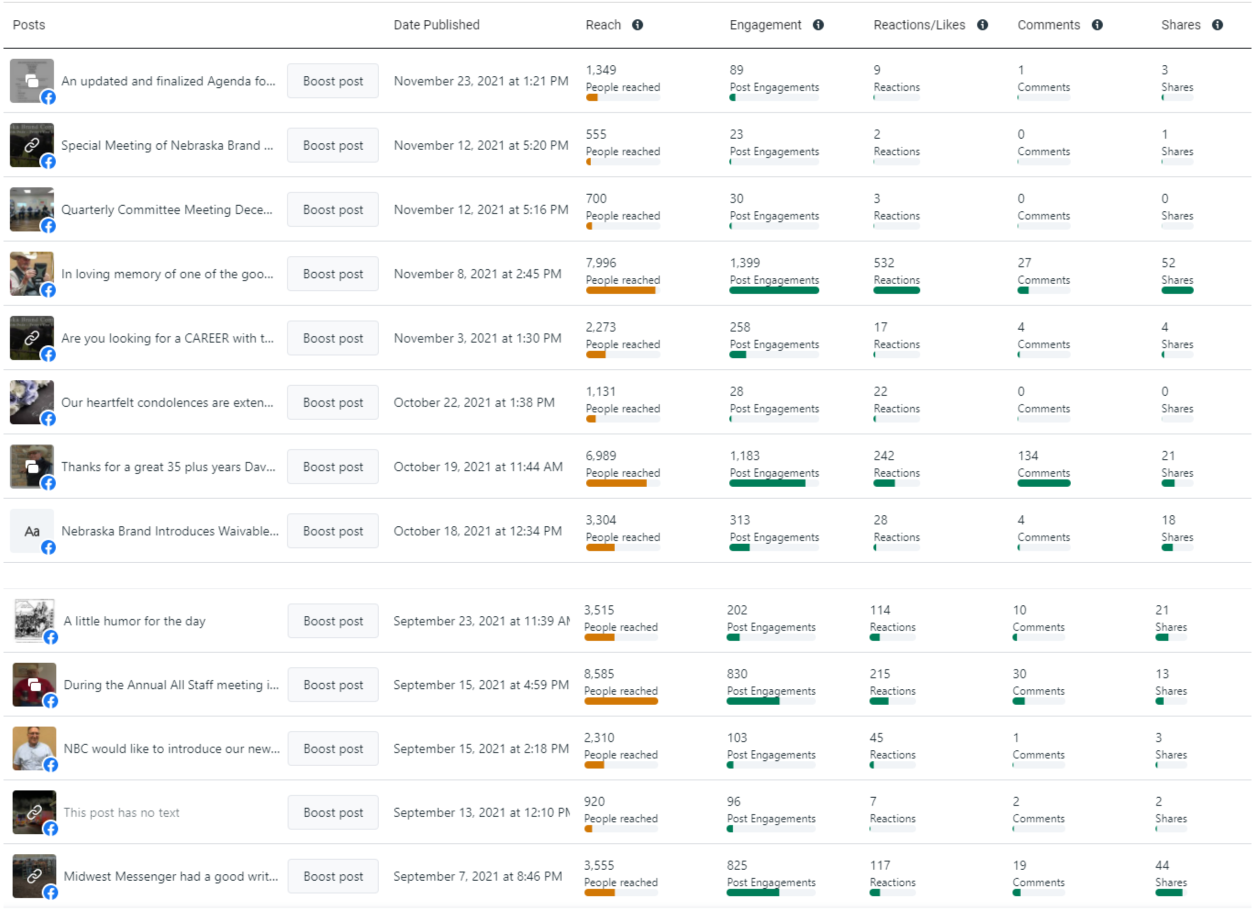
- Confirmed advisory group which has subsequently been renamed as the E-Inspection Subcommittee. I am very pleased with the producers who have volunteered to represent this topic and believe they will be great selections.
- Have now had 2 subcommittee meetings on Nov 2nd and Nov 19th. Both were in person with 60% and 70% attendance at the Thedford NRD office.
- Next meeting is scheduled for online Webex on December 17th.
- Working on preliminary contracts with CattleProof to present to Committee in the near future.
- Finalizing contract and negotiating pricing for E-Inspection and portal costs with NIC.
- Met with both NI and CattleProof development teams in Lincoln on Sept 16th. Went over the challenges, process, and next steps while the dev teams brainstormed a way to proceed.
- Legislative Update Report has been completed, approved and will be sent On Nov 30th to satisfy Dec 1 deadline.
- Legislative update to be presented to Ag Committee December 9th.

**Additional tasks**

- Ongoing solicitation and posting in local Ogallala area to drive applications for inspectors.
- Created multiple press releases which are sent to 40 publications regarding new legislative changes. Committee member Tanya Storer assisted and approved some releases.
- Ongoing posts to our social media Facebook account
- Continually building and updating hardware and devices for new staff and outgoing staff
- Working on completing the updated Procedures Handbook and updating most forms to an electronic format and updated format when time permits.
- Ongoing support of field staff and supervisors and office personnel.

Data Analytics

Facebook posts for the last quarter:



| Posts | | Date Published | Reach | Engagement | Reactions/Likes | Comments | Shares |
|---|---|---|---|---|---|---|---|
| An updated and finalized Agenda fo... | Boost post | November 23, 2021 at 1:21 PM | 1,349<br>People reached | 89<br>Post Engagements | 9<br>Reactions | 1<br>Comments | 3<br>Shares |
| Special Meeting of Nebraska Brand ... | Boost post | November 12, 2021 at 5:20 PM | 555<br>People reached | 23<br>Post Engagements | 2<br>Reactions | 0<br>Comments | 1<br>Shares |
| Quarterly Committee Meeting Dece... | Boost post | November 12, 2021 at 5:16 PM | 700<br>People reached | 30<br>Post Engagements | 3<br>Reactions | 0<br>Comments | 0<br>Shares |
| In loving memory of one of the goo... | Boost post | November 8, 2021 at 2:45 PM | 7,996<br>People reached | 1,399<br>Post Engagements | 532<br>Reactions | 27<br>Comments | 52<br>Shares |
| Are you looking for a CAREER with t... | Boost post | November 3, 2021 at 1:30 PM | 2,273<br>People reached | 258<br>Post Engagements | 17<br>Reactions | 4<br>Comments | 4<br>Shares |
| Our heartfelt condolences are exten... | Boost post | October 22, 2021 at 1:38 PM | 1,131<br>People reached | 28<br>Post Engagements | 22<br>Reactions | 0<br>Comments | 0<br>Shares |
| Thanks for a great 35 plus years Dav... | Boost post | October 19, 2021 at 11:44 AM | 6,989<br>People reached | 1,183<br>Post Engagements | 242<br>Reactions | 134<br>Comments | 21<br>Shares |
| Nebraska Brand Introduces Waivable... | Boost post | October 18, 2021 at 12:34 PM | 3,304<br>People reached | 313<br>Post Engagements | 28<br>Reactions | 4<br>Comments | 18<br>Shares |
| A little humor for the day | Boost post | September 23, 2021 at 11:39 AI | 3,515<br>People reached | 202<br>Post Engagements | 114<br>Reactions | 10<br>Comments | 21<br>Shares |
| During the Annual All Staff meeting i... | Boost post | September 15, 2021 at 4:59 PM | 8,585<br>People reached | 830<br>Post Engagements | 215<br>Reactions | 30<br>Comments | 13<br>Shares |
| NBC would like to introduce our new... | Boost post | September 15, 2021 at 2:18 PM | 2,310<br>People reached | 103<br>Post Engagements | 45<br>Reactions | 1<br>Comments | 3<br>Shares |
| This post has no text | Boost post | September 13, 2021 at 12:10 PI | 920<br>People reached | 96<br>Post Engagements | 7<br>Reactions | 2<br>Comments | 2<br>Shares |
| Midwest Messenger had a good writ... | Boost post | September 7, 2021 at 8:46 PM | 3,555<br>People reached | 825<br>Post Engagements | 117<br>Reactions | 19<br>Comments | 44<br>Shares |

# Nebraska Brand Committee

# Electronic Inspection Project
# Legislative Report

December 1, 2021

Prepared by Danna Schwenk

NBC Technology Coordinator/Project Manager

# Contents

The Nebraska Brand Committee is committed to implementing the changes passed in LB 572 earlier this spring. Included in that is the voluntary Electronic Inspection, or E-Inspection, option for producers looking for a different and expediated method of brand inspections versus the gold standard of the hot iron or freeze brands.

## The Need for E-Inspection

Of the more than 3 million cattle that are inspected through Nebraska local and sale barn inspections each year about 45% of the cattle have no hot iron or freeze brand applied, making them a slick hided or "no-brand" animal. We have several segments of our industry that prefer not to hot iron brand at all but choose to use electronic identification as their means to identify an animal. We do know over 2 million EID tags are already in use in Nebraska (2019 data) and more are being used each year as value added programs and USDA Brucellosis e-tagging increase in popularity. It was from a combination of these facts that the E-Inspection option came to light in 2018 after analyzing the first year's data collected from the new computerized inspection system on percentage of No Brand animals inspected. Prior to 2018 this data had never been available to review.

Over the following two years, staff was charged with originating an outline of how inspections could be performed using electronic identifiers and evaluating other similar programs. During this time the Committee members identified several reasons why this program could be beneficial for both producers and the NBC:

- Simplify the inspection process for producers that utilize EID's
- Eliminate travel expenses or surcharges for an inspector's physical appearance
- Provide a value-added service for those that use EID's already
- EID's provide more identification on non-branded cattle than those without
- Should be able to create a reduced charge compared to physical inspection
- Could be used to accommodate dairy shipping certificates
- Could promote participation in Animal Disease Traceability system for state of Nebraska and USDA

After the original program conception was determined and initial research was conducted, it was decided internally that a producer advisory group would be extremely beneficial in vetting ideas, requirements and processes put forth by the staff. This is a common practice prior to specification or development occurring. The focus of the E-Inspection Subcommittee is to provide insight to the NBC staff as to how an electronic inspection program could work for each of the different producer types while maintaining the integrity of the Brand Laws.

This information will serve as the foundation for a system that we believe will create greater efficiencies by minimizing field staff travel and time; decrease producer expenses; reduce scheduling conflicts for producers; improve ease of timely document generation; be able to add value on existing EID usage at operations; and streamline the inspection process for non-change of ownership and eventually change of owner movements.

While this is the first major change to Brand Inspection law since its inception in 1941, NBC believes this can be done by taking an approach that utilizes our new computerized inspection program allowing producers access through a web-based producer portal to generate their own "inspections" using EID's as legal evidence of ownership. There will be requirements on what cattle are included and when the E-Inspections can be performed, with enrollment of eligible cattle a corner stone of the program. Data integrity will be verified automatically through the system with incomplete or questionable animals and transactions flagged for human auditing and validation.

NBC understands that this is a very progressive and complicated program that has many in the industry concerned that it undermines the integrity of the Brand Law. NBC strives to assure producers that any program implemented would have as high if not higher requirements that current hot iron branding inspections has. This program does not intend on any level to replace or eliminate hot iron or freeze branding as the main form of identification in Nebraska and is intended to be completely voluntary for producers that find the benefit in using it.

# The Plan

The development of this program will involve many steps and milestones as we build and implement it from ideas, to design, to development, to testing then into use. Timelines can not be determined until development specifications are completed and reviewed. Some phases can run concurrently. These are medium level details and are subject to change as rules and processes are finalized.

## Phase I – Conceptualization

This will include the previous two years of outlines, brainstorming, evaluating other state systems, USDA programs, current industry accepted programs, investigating data systems, learning more of blockchain pro's and con's, and finally settling on a solid foundation of how the system will work and which components are selected. This includes the formation of the E-Inspection Subcommittee and their input.

1) Program Outline created
2) Data storage determined
    a. Legal determination on need for 3rd party animal database being obtained
3) Sections identified
4) Providers selected
    a. Contracts being drafted for Committee approval
5) Subcommittee confirmed and conducting meetings
    a. Need to finalize rules and details of program for both enrollment and inspection
    b. Audit requirements need to be finalized

## Phase II – Specifications

Once we have more specific details the remainder of the specifications will be written and passed to the development team for creating development stories and estimations of development, testing and quality assurance (QA) capacity and time. This will need to occur across all platforms and systems being used.

1) Producer Portal Access
    a. Preliminary specifications completed in 2020
2) Individual Animal Database
    a. Has been developed and is in testing for basic requirements
3) Interface created between the two with an API (Application Programming Interface)
    a. Development companies have met and outlined preliminary requirements while waiting on final rules.

## Phase III – Preliminary Alpha use

There will be parts of Phase II that are completed enough to start using the Producer Portal and potentially for enrollment of cattle into the program.

1) Producer Portal use:
    a. Initial items as updating producer information and brands, renewing brands, and reviewing all inspections on record since 2018.
    b. Initial Producer access development completed and in testing in 2021
    c. Expected release for first Producer Portal tasks in early 2022 of brand renewal, data updating and inspection lookup to be included.
2) Animal ID data system:
    a. Enrollment of animals and review who is enrolled
3) Electronic Inspection Milestone 1 – Non change of owner
    a. Will be spec'd out and developed during this phase using both pieces listed above in beta testing
    b. Non change of owner inspections
4) Data API will be developed and tested
5) Data import features will be built

## Phase IV – Beta User testing and ongoing enhancement development

With the initial system up and running additional components will be finished with development that will allow the test group of Beta users to work through preliminary usage and help revise and refine the best physical process of the system. This will also be when the auditing and automatic Animal Disease Traceability reporting to the state Veterinarian system occurs and the next Inspection Milestone development is completed.

1) Preliminary test use of e-inspection for non-change of ownership transactions
2) Audit rules specifications will be developed and tested
3) ADT reporting interface created
4) Electronic Inspection Milestone 2 - COO
    a. Change of Owner Inspections will be spec'd out and developed during this phase

5) Partner discussion on how to make interstate inspections a reality and specifications written

### Phase V – Implementation of title transfer Inspections

Beta users will be able to test the change of ownership inspections, will complete the dairy calf shipping certificates (same principles used for change of ownership e-inspection) and will develop sale barn E-Inspections

1) Milestone 2 – Change of Owner inspections development completed and in testing
    a. Dairy shipping certificates completed
2) Milestone 3 – Sale Barn inspections will be determined, and specifications created
3) Development of enhancements for interstate inspections process by partner states

### Phase VI – Implementation of Sale Barn transfers

1) Milestone 3 – Sale Barn inspections completed and in testing
2) Implementation of interstate inspections process by partner states

## The Technology

While the Plan gives a more specific overview of the order that we would expect the project to take, there are details that are important to the project and producers that we learned in the first two years of investigating this project.

Data integrity, security and privacy were by far the most concerning elements. In order to alleviate these, it was decided to utilize a 3rd party system that would ensure that all individual animal information was kept as private as possible. It is believed with a 3rd party system that is not “owned” by the State of Nebraska the data cannot therefore be accessed with a Freedom of Information Act (FOIA) request. This is being confirmed by the NBC legal team. With an independent provider it will also enable all users to agree to an End User License Agreements (EULA) that specifically details what information can be used, shared or provided to different partners and when.

Regarding data integrity, NBC opted to utilize the newer technology of Blockchain that offers several benefits over a standard database system.

1. Trust between different entities without relationships that do data sharing
2. Decentralized structure which means all along the chain no one is exclusively in charge.
3. Which means blockchain enables unprecedented control over users own data, with limits and permissions enforced by blockchain enabled smart contracts.
4. The enhanced security offered by blockchain stems from how Blockchain creates an unalterable record of transactions with end-to-end encryption, which shuts out fraud and unauthorized activity.

5. Data on the blockchain is stored across a network of computers, making it nearly impossible to hack (unlike conventional computer systems that store data together with servers).
6. Blockchain addresses privacy concerns better than traditional computer systems by anonymizing data and requiring permissions to limit access.
7. Immutability. Once recorded on blockchain data cannot be changed or deleted. It creates a permanent date/time stamped record creating a secure reliable audit. It can't be corrupted or retired.

Because we are dealing with animal records that should not ever be changed, immutability is the biggest factor when opting for a blockchain ledger system. Finding companies that work with blockchain in the agriculture sector wasn't difficult, however finding ones that would work in our space and budget was another issue. After interviewing and demoing over 10 different suppliers over 2 years, the option to work with CattleProof as our 3rd party animal database was settled upon.

CattleProof offers several different services, but the core NBC requirement is use of the animal record and its interface capability with Nebraska Interactive and our NBC Admin Producer Portal program. The CattleProof system creates a verified digital identity for individual animals that can be used for any program that producers choose to participate in.  It becomes the trusted repository for all verified data and documentation. CattleProof utilizes Ethereum blockchain provenance but has the ability to be interoperable with other chains based on cost and data needs.

CattleProof contracts are being drawn up and will be available for the Committee to review very soon.

NIC (formerly Nebraska Interactive) is the company that provides our NBC Admin program that handles all of our producer data, inspections, brands and financial transactions relating to all brand and inspection transactions.  NIC also builds and managers our internet website content. Our initial contract for producer and inspection services did not include financial compensation for building projects outside the original and even renegotiated scope.  As this is a major development endeavor, a new contract is also being negotiated to allow for us to build and support the Portal and E-Inspection projects.

The new NIC contract is currently in ongoing negotiations and should be finalized soon.

## The Process

NBC staff drafted the first preliminary outline of the proposed project.  After that NBC investigative and management staff was then included to understand and assist in modeling the program to fit within the constraints of the Brand Act itself. With the preliminary structural requirements in place, it was now time to engage producer users to help refine the requirements and processes that could be used in agreement between law and practicality.

## E-Inspection Subcommittee

Once LB572 was signed into law, the NBC staff has been trying to identify and confirmed 10 producers in the brand inspection area that would represent almost every facet of cattle production to participate on an advisory team that would become the E-Inspection Subcommittee. These producers have been selected based on the grounds of their progressive operations and use of or planned use of electronic identifiers in their operation. Over 20 producers were recommended and engaged by Brand staff during this time. As a point of clarification, the participants were selected based not on any membership or affiliation (except for their industry segment), but strictly from suggestions and reviews from other producers and industry experts familiar with the producers and their situations.

Current participants and their segments include:

- Cory Banzhaf, JKS Farms, Pleasanton, feeder/cow-calf
- Art Brownlee, JHL Ranch, Ashby, commercial with retained ownership to harvest
- Jed Connealy, Connealy Cattle, Whitman, Seedstock & grow yard
- Chris Finney, Ainsworth Vet Clinic, Ainsworth, Veterinarian & Backgrounder
- Kim Ford, Cross Diamond Cattle Co, Bertrand, Seedstock
- Jill Krajewski, Oshkosh Heifer Development, Oshkosh, Dairy heifer development/cow-calf
- Gabriel Monasterio, Wolf Cattle Company, Ainsworth, seedstock/commercial/feeder
- Jay Nordausen, Ogallala Livestock Auction Market, Ogallala, Sale Barn
- Sherry Vinton, Vinton Ranch, Whitman, commercial cow-calf
- Steve Wolf, Wolfden Farms, Kearney, NE Holstein Association & dairy producer

With the directive of a legislative update by December of 2021, the Subcommittee was able to meet in person on November 2nd for the first in a series of sessions to meet the group, learn more of the tentative processes outlined, how it could work, where specific hurdles have been identified to work though and what the next steps are in creating a preliminary plan for E-Inspection. Once the plan has been firmed up, it can then be brought before all producers for additional comments and to answer questions that might arise.

After the second in person meeting on November 19th, the subcommittee members have a clearer understanding of the significance of maintaining the integrity of Brand Law. While each of the different members individually can see a way forward, to be able to make E-Inspection advantageous for all is more challenging. Some of the main discussion points for the preliminary set of topics have pertained to the 3rd party animal database, tag types being used, different enrollment options, rules of inspections to align with brand law, expanding eligibility outside of brand area, auditing process and much more.

The next meeting will occur virtually in the middle of December with a 4th to be planned for early January to ensure timely forward progress. It is incumbent upon NBC and the subcommittee to spend as much time as necessary to get this program correct instead of rushing it to market. It was decided by the Committee that the E-Inspections will start with non-change of owner transactions as our initial Milestone, and then move to change of owner title transfers once the process is tested and perfected, and then look at the possibility of Sale Barn E-Inspections.

## Functional Process

At this point in time a preliminary general process has been established but is currently being reviewed and adjusted by the Subcommittee.

*All information in this following section is subject to change.*

1. Producers will be registered and have access to the NBC Producer Portal
2. All cattle must be enrolled prior to an E-Inspection occurring.
3. Producers initiating the movement or sale will create the E-Inspection
4. Producer will read animal ID's and records those records to individual animal database through a transaction record
5. Producer uploads any accompanying required documentation
6. Payment occurs online prior to transaction completion
7. System performs a validating audit of animal records
8. Approval of transactions occurs in minutes, but NBC has 48 hours to completely audit and approve in case of flags from automated validation.
9. Producer is notified that documents are available and can be printed.
10. Title of ownership on EID record then transfers to new owner.

## Enrollment

Enrollment of cattle will be mandatory for participation of E-Inspections. At this time there are 4 preliminary enrollment types that have been identified:

- Breeder Enrollment – cattle are at the initial breeder or owner and will require documentation to verify this.
- Inspection Enrollment – Cattle were physically inspected at the time of enrollment.
- Documented Enrollment – Cattle were physically inspected at the time of enrollment through a similar state inspection or sale barn as Nebraska.
- Registered Enrollment – cattle are enrolled when originally tagged at place of birth with approved documentation and proof of ownership

# Next steps

The Subcommittee has contributed greatly and has been very engaged, but we are left with outstanding discussion points for the preliminary set of topics that need confirming including:

- Understanding the 3rd party individual animal system that would interface with the inspection system
- Does the animal database need to be 3rd party for FOIA issues or if subcontracted by NBC makes that irrelevant
- Should the system use only 840 tags or be open to any approved ICAR RFID (ISO 11784 and 11785)
- Will premise numbers be required if 840 is used
- Working though the proposed various enrollment options and perhaps adding a 4th option for a registered herd which could prove ownership
- Potentially using vet information/receipts to prove cow herd numbers for breeder enrolling
- Will maternal enrollment be required for breeder enrollment option: pros/cons
- Enlarging geographic area for document enrollment outside of Nebraska and Brand Area
- Potential for creating a registered E-Inspection operation and statute pitfalls
- Understanding that documents that satisfy PVP participation don't necessarily equate to cattle ownership validation
- Secondary identifiers should be a requirement for EID
- Evaluating the time frame for reading cattle tags that equal the shipment head count.
- How the auditing process could work

Once we have these items finalized, specifications should be able to be generated.

# Area II Quarterly Report

**Criminal Investigator Thomas Hughson**

**December 1, 2021**

**Open Investigations:**

- Sheridan County – Bankruptcy/Brand violations - Solved
- Banner County - Theft
- Sioux County – Bankruptcy/ share dispute
- Sheridan County – Assisting a Federal investigation
- Dawes County – Neglect – solved
- Box Butte County – Theft
- Keith County - Theft

**Court Cases:**

- none

**Violations:**

- Worked violation inspections. Colorado, South Dakota & Wyoming.
- Worked 5 violation resulting from a sale without inspection.
- Worked with Colorado cattle shipped without inspection.
- Worked with South Dakota cattle shipped without inspection.
- Working numerous violations in Sioux and Garden County.
- Worked 3 violation inspections at Torrington Livestock.

**Estray Cases:**

- Several solved pending paper work.

Truck Checks: 0

**Grazing Permits:**

- **Continual approval and questions.**

**Continuing Education:**

- **Kearney Sheriffs convention**

**Employee interaction:**

- **There has been considerably more employee interaction this quarter. My transformation into the chief position has changed how my days, weeks and months look. I have been trying to spend at least 2 days a week in the Alliance office handling producer question and working closely with the team there on coverage due to recent resignations in the west area. I have also been traveling more and getting a feel for more than just Area II.**
- Grazing Permits
- Inspection requirements
- Health Requirements
- Out of state permits
- Horse issues
- Open Markets
- Brand Transfers
- Divorce/Division of assets.
- Banks – sales records/ proof of ownership.

## AREA INVESTIGATORS QUARTERLY REPORT

**QUARTER: 2 MONTH: December of 2021 FISCAL YEAR: July 2021 – June 2022**
**AREA: III INVESTIGATORS NAME: C. Fell**

## INVESTIGATOR OVERVIEW:

It has been a busy quarter with violations and estrays coming in. Pulled a major theft case in North Platte that took me to Kansas and has had me working with Tennessee, Missouri, and Kansas investigators.

## TOTAL # OF INVESTIGATIONS/ THEFT/ ASSOCIATED CRIMES, ACTIVE/ CLEARED OR UNFOUNDED: 07

| CASE# | VIOLATION: | COUNTY: | DISPOSITION: |
|---|---|---|---|
| 091421CF3 | AOA estray | Franklin | Owner Located |
| 091321CF3 | Producer issues | Dawson | Active |
| 092121CF3 | Theft | Lincoln | Active |
| 101521CF3 | AOA Neighbor Issues | Furnas | S. O. Handled |
| 101521CF3 | Missing/theft | Harlan | Cattle Located |
| 102021CF3 | Neighbor issues | Hitchcock | Cattle Returned |
| 110121CF3 | Trespassing L/S | Webster | Active |

## COURT CASES PENDING: 04

| DATE: | VIOLATION: | COUNTY: | DISPOSITION: |
|---|---|---|---|
| 030420CF3 | Felony Selling to avoid Lien | Adams County. | Charges Filed |
| 110321CF3a | Felony Theft by Deception | Lincoln County | Charges Filed |
| 110321CF3b | Felony Prohibited sale of L/S | Keith County | Charges Filed |
| 110321CF3c | Assist - Felony Theft | Dodge City Kansas | Charges Filed |

**WARNING TICKETS ISSUED: 00**

| DATE: | ADDRESS: | COUNTY: | VIOLATION: |
|---|---|---|---|

**TOTAL VIOLATIONS: 08**

**VIOLATIONS HANDLED BY WRITTEN OR VERBAL WARNING: 00**

| DATE: | ADDRESS: | COUNTY: | VIOLATION: |
|---|---|---|---|

**VIOLATION INSPECTIONS: 00**

**VIOLATIONS TRANSFERRED TO OTHER STATES: 00**

**VIOLATIONS PENDING ACTION: 08**

| CASE# | VIOLATION: | COUNTY: | DISPOSITION: |
|---|---|---|---|
| 092120CF3v | 54-1,110 | Dawson | |
| 080920CF3v | 54-1,111 | Lincoln | |
| 010521CF3v | 54-1,111 | Perkins | |
| 052021CF3v | 54-1,111 | Perkins | |
| 082021CF3v | 54-1,110 | Lincoln | |
| 082021CF3v | 54-1,110 | Lincoln | |
| 083021CF3v | 54-1,110 | Lincoln | |
| 092121CF3v | 54-1,110 | Lincoln | |

**TOTAL ESTRAY CASES: 06**

**HOLDS ASSISTED WITH PRIOR TO BECOMING ESTRAY CASES: 02**

| DATE | LOCATION | HD. COUNT | DISPOSITION |
|---|---|---|---|
| 071621 | Lexington | unknown | Hold Cleared |
| 111521 | Imperial | 3 | Owners Located |

**ESTRAY CASES SOLD BY THE NEBRASKA BRAND COMMITTEE: 06**

| CASE#: | DATE RECEIVED: | SOLD AT: | HD. COUNT: | DISPOSITION: |
|---|---|---|---|---|
| 5456 | 022820 | McCook | 1 | Active |
| 5463 | 020320 | N. Platte | 2 | Active |
| 5475 | 072020 | Alma | 1 | Active |
| 5478 | 082520 | N. Platte | 1 | Active |
| 5492 | 020121 | N. Platte | 1 | Active |
| 5499 | 030121 | Imperial | 1 | Active |

Received 7 new cases in past week that need numbers attached.

## TRUCK CHECKS PERFORMED BY INVESTIGATOR:

| DATE: | Location | #of Contacts | #of Livestock | #Written/Verbal | #Inspections |
|---|---|---|---|---|---|
| 090921 | Merriman | 2 | 1200 | 0 | 0 |

## TOTAL# OF CLASSES OR PRESENTATIONS GIVEN: 02

None

## EMPLOYEE SUPERVISION

None

## PRODUCER ISSUES:

Normal Producer Questions, Mostly about Estrays

Grazing Permits,

Inspection Requirements,

Health Requirements,

Out of State Permits,

Horse Issues,   From Colorado Inspector

Open Markets,

Brand Transfers,

Divorce/ Division of Assets,

Banks: Sale Records, Proof of Ownership.

## REGISTERED FEEDLOT AUDITS: 08

Eight RFL's to Audit currently. One New RFL was added in Dundy County this quarter.

## TECHNOLOGY & TRAINING:

Attended Sheriffs Convention

## PUBLIC RELATIONS & EDUCATION:

Western States Livestock Rural Enforcement Association (WSLREA) State Rep. Monthly conference calls about annual March training conference. March 2022 Meeting will be held March 1-3 2022 at the Silver Legacy resort in Reno, NV.

**INVESTIGATORS SIGNATURE:** ____________________

## SEPTEMBER, OCTOBER, NOVEMBER 2021 QUARTERLY REPORT

## AREA 4

## INV. BRENT DEIBLER #8904

TRUCK CHECKS:

09/01/21 GRANT

10/26/21 ALLIANCE

09/09/21 MERRIMAN

REGISTERED FEED YARD CHECKS:

DEIBLER HAS BEEN ISSUED 17 RFL CHECKS TO WORK IN AREA 4. ALL RFL CHECKS UP TO END OF NOVEMBER ARE CURRENT FOR THE QUARTERLY CHECKS OF 2021.

DEIBLER HAS NUMEROUS VIOLATIONS AND ESTRAY CASES TO WORK FROM BRAND ISPECTORS.

UPDATE ON CASES AND DAILY PROJECTS:

09020121BD4: POSSIBLE STOLEN CATTLE IN HOLT COUNTY. CLOSED

09160121BD4: DROVE TO SCRIBNER AREA TO FINILIZE ESTRAY CASE. CLOSED

09200121BD4: ASSIST HOLT COUNTY BRAND INSPECTOR WITH INSPECTION OF CATTLE FOR SALE AT BARN. CLOSED

09200221BF4: ASSIST BUFFALO COUNTY BRAND INSPECTOR WITH LOUP CITY SALE BARN ISSUES. CLOSED

09210121BD4: ASSISTED HOWARD COUNTY SHERIFF'S OFFICE WITH MISSING CATTLE, POSSIBLE STOLEN FROM LOCAL FEEDYARD. OPEN

09210221BD4: ASSISTED HOLT COUNTY BRAND INSPECTOR WITH OUT OF STATE CATTLE PROOF OF OWNERSHIP ISSUES. CLOSED

09210321BD4: ASSSISTED BOYD COUNTY SHERIFF'S WITH ESTRAY CATTLE RUNNING IN COUNTY. CLOSED

10010121BD4: ASSISTED GAME AND PARKS WITH A FERAL HOG PROBLEM IN NORTHEAST NEBRASKA. OPEN

10030121BD4: COMPLAINT OF NEGLECT CATTLE IN CUSTER COUNTY, DID FOLLOW UP WITH SHERIFF'S OFFICE. CLOSED

10050121BD4: ASSISTED HOLT COUNTY BRAND INSPECTOR WITH MISS BRANDED OUT OF STATE CATTLE. CLOSED

10050221BD4: ASSISTED CUSTER CCOUNTY SHERIFF'S OFFICE WITH IDENTIFYING AN INDIVIDUAL USING BRAND COMMITTEE ISSUED LAW ENFORCEMENT SEARCH ENGINE. OPEN

10120121BD4: ISSUED VERBAL WARNING AND EXPLAINED BRAND LAW TO SMALL PACKING HOUSE IN HOLT COUNTY. CLOSED

10140121BD4: ASSISTED HOLT COUNTY BRAND INSPECTOR WITH CATTLE LEAVING AREA WITH OUT INSPECTION. CLOSED

10150121BD4: ASSISTED ROCK COUNTY BRAND INSPECTOR WITH POSSIBLE ESTRAY CASE. OPEN

10180121BD4: ASSISTED BOYD COUNTY SHERIFF'S OFFICE WTH HIT AND RUN ON TWO HEAD OF CATTLE ROADSIDE. OPEN

10190121BD4: ASSISTED SOUTH DAKOTA BRAND ISPECTOR WITH IDENTIFYING BRAND. CLOSED

10210121BD4: DROVE TO SUPERIOR TO MEET WITH PRODUCER ON BRAND LAW VIOLATION. OPEN

10250121BD4: ASSISTED CHERRY COUNTY BRAND INSPECTOR WITH CATTLE LEAVING AREA.

10260121BD4: VIOLATION ISPECTION ON CATTLE LEAVING AREA FROM BURWELL AREA. CLOSED

10270121BD4: COMPLAINT CATTLE ON NEIGHBORS GROUND ON GOING PROBLEM. OPEN

10280121BD4: ASSISTED ROCK COUNTY BRAND INSPECTOR WITH GETTING TRUCKS STOPPED TO DO VOILATION INSPECTION. CLOSED

10290121BD4: DROVE TO CLARKS AREA WITH BRAND INSPECTOR TO COMPLETE VIOLATION INSPECTION. CLOSED

11040121BD4: DROVE TO FULLERTON AREA WITH BRAND INSPECTOR TO PERFORM VIOLATION INSPECTION. CLOSED

11230121BD4: ASSISTING HOLT COUNTY BRAND INSPECTOR WITH PROOF OF OWNERSHIP ON CATTLE AT SALEBARN. OPEN

11240121BD4: ASSISTED KNOX COUNTY DEPUTY WITH POSSIBLE STOLEN CATTLE CASE. OPEN

DEIBLER SPENT FEW DAYS IN KEARNEY TO ATTEND THE STATE SHERIFF'S CONVENTION. CONTINUES HOURS FOR TRAINING WERE DOCUMENTED FOR HOURS OF SERVICE TRAINING IN DEIBLER'S FILE. DEIBLER WAS QUAILIFIED ON AN "AR" STYLE RIFLE FROM ROCK COUNTY DEPUTY TO STAY QUALIFIED WITH THE TRAINING ACADEMY REQUIREMENTS.

DEIBLER HAS ASSISTED NUMEROUS BRAND INSPECTORS WITH CATTLE LEAVING THE AREA WITHOUT INSPECTION. THERE HAS BEEN SEVERAL GROUPS OF CATTLE CHECKED BECAUSE OF GOOD COMMUNICATION AND TEAM WORK FROM INSPECTORS AND INVESTIGATORS!

NEBRASKA BRAND COMMITTEE

Post Office Box I • 411 Niobrara Ave.
Alliance, NE USA 69301-0775

INSPECT • RECORD • POLICE

# Chief Inspector – Quarterly Report

**December 2021**

The majority of my time has been spent focusing on the west area, with the shortage of inspectors in that area, specifically the Ogallala area. We have had one new hire for Ogallala, Bryce Davis, who is doing an exceptional job. We also moved Jeremy Kennedy to full time in the Crawford area. The crew we do have in the west area has done a great job of stepping up and doing what needs to be done during this shortage, along with help from the south area, that has been greatly appreciated.

Before the west took priority, I did manage to visit all of the west and south sale barns, as well as Broken Bow and Kearney in the east area. I also visited Tyson and Gibbon pack during this time.

My time not spent on scheduling and assisting in the west area has been spent on phone calls and emails from producers, supervisors and inspectors, Interviews, working with the leadership team on ways to improve the Brand Committee, assisting Danna with some dealings with our various tech partners, EID meetings and my continued financial duties.

One of our steps forward as a leadership team was the implantation of our temporary area leads. This will hopefully relieve some of the pressure in the west and free us up in some of our options in trying to fill the remaining positions in the west.

It has been an interesting and fast paced first month in the new position, as I work to find the balance of the Inspector and the financial portions of the position, that I hope to continue to grow and improve in as I tackle this new position.

NEBRASKA BRAND COMMITTEE

Post Office Box I • 411 Niobrara Ave.
Alliance, NE USA 69301-0775

INSPECT • RECORD • POLICE

# December 2021

## Quarterly Report – East

### RFL

_I have all my registered feedlots caught up and have no issues. The paperwork issue with feedlot cows for Gibbon Pack has been resolved.

### Personel Changes

We have hired 3 new inspectors at Kearney. We have hired Sarah McGown, Josh Cox and Tryssta Duvel as inspector trainees. At this time we are fully staffed.

### Salebarn visits

_I have been busy going to Kearney assisting Mckenzie with new hires on sale days at Huss. I have been at Broken Bow almost every Thursday to assist and monitor Richard Estergards progress. Richard is doing well and gaining confidence every day. I have been to Ericson, Albion and Burwell salebarns to check in on staff and help when they have been short on help. I have been covering locals during the fall run when needed. Everyone has been busy and working hard to keep cattle moving. I plan on going to Gibbon Pack as soon as possible. They had a covid positive person in the pens and some of the people I need to visit with are on 14 day quarantine. I have been answering phone calls and questions by staff daily. I have been helping staff with lining up help when needed. So far the comp time has been manageable as the locals have slowed a bit but the salebarns are starting to get larger runs.

### Testing

I have 2 inspectors that will be due to take some tests starting in December to monitor there progression and the areas we need to work on. I will have several employees in the next coming months going through this testing also.

Shawn Hanks
East Area District Supervisor
Nebraska Brand Committee
shawn.hanks@nebraska.gov

# North District Supervisor Quarterly Report

## *Kayla Jesse*

***RFLs***

RFLs, continue to be caught up and on track with the scheduled Audits.

Monthly Audits at Adams Land and Livestock

***Personal Changes***

We have had some changes up here in the Northern area, but happy to say and knock on wood, we are fully staffed now. Sam Day went from full time in the Valentine area to intermittent. We got Mari Smith from the Kearney area to take his position, that is going very well and happy with the transition. Kevin Meyer was hired as an Intermittent, he started October 1st and is doing very well. Zane Snyder was intermittent in the Boyd Co area. He retired from South Dakota Brand Board and we were able to put him into a full-time position. That has been very helpful.

***Day to Day*** .

Helping the inspectors keep an eye on their comp time hours and moving people around where needed.

Have had many calls and questions from not only the inspectors, but from producers asking about laws and movement of cattle, keeping my inspectors educated and refreshed on these issues has helped a ton.

Fall Run was very busy for us, I jumped in where I was needed for scheduling conflicts and last-minute inspections, the 48 hour notice has been received well. It has been a great tool for us to use with producers who may neglect to think ahead of time and are habitual about it.

visiting Sale Barns and inspectors

keeping an eye on inspectors hours and mileage vouchers

taking phone calls for help with IT issues and other employee questions.

Committee meeting in Kearney Dec 1, 2021

**NEBRASKA BRAND COMMITTEE**

Post Office Box I • 411 Niobrara Ave.
Alliance, NE USA 69301-0775

**INSPECT • RECORD • POLICE**

# South – Quarterly Report

**December 2021**

## Employment

- Two full time new hires in September – Lexington: Shea Goddard & Lindsey Jack
- One Intermittent new hire in September - Stratton area: Erin Korell
- Helped East area with an interview
- North Platte's Sustainable Beef packing house is furthering its process to break ground

## Training

- Continually working with inspectors in my area in all aspects
- Have Supervisor conference calls weekly
- Nebraska Interactive conference calls/zoom meetings regularly
- Built a couple new hire iPads
  - Placed KS & SD brand book on all new iPads and just recently learned CO brand book is now available
  - Added 7 forms to all new iPads for easy 'fill and sign' or print and fill out
- Attended two E-Inspection Sub Committee meetings

## Visits / Inspections

- Visited Ogallala, Lexington, North Platte, Alma, Imperial, and McCook sale barns
- Completed 23 Registered Feedlot Audits
- Still 'dispatching' locals
- Have received calls that required more in Investigative work – forwarded to Inv Fell
- South area workload has been steady – especially around the North Platte area
- Kept pending cash payments to minimal
- South Area gained an RFL
- Recovered 8 strays

## Personnel

- Email inspectors to keep them informed
- Continually answering calls, texts, and emails
- Assist with clearing Holds and Pending Payments
- Deal with personnel issues
- Reviewing/approving expense vouchers and Vacation requests
- Work together with the other District Supervisors to best serve the Brand Area
- Answer calls/questions from inspectors within each of the areas
- Keeping comp time hours to reasonable amount

Kortnie Shafer
South District Supervisor / Asst IT Corrdinator
Nebraska Brand Committee