State of Nebraska INCIDENT RESPONSE FORM

This form is based on the State of Nebraska Incident Response Standard, which agencies are required to use when reporting an incident. An automated version of this form can be found at ??????????. For urgent assistance, contact the State Information Security Officer at (402) 471-7031 or 416-3668.

1. Point of Contact Information for this Incident:

Name:	Agency:
Phone:	Cell/Pager:

2. Physical Location of Affected Computer/Network:

(include building number, room number, etc)

3. Date and Time Incident Occurred and Duration:

(mm/dd/yy)	(hh:mm:ss am/pm)	Duration:

4. Type of Incident (check all that apply):

☐ Intrusion	☐ Access Control Avoidance
☐ Denial of Service	☐ Unauthorized Access
☐ Virus / Malicious code (complete 4a)	☐ User Account Compromise
☐ System Misuse	☐ Hoax
☐ Social Engineering	☐ Network Scanning / Probing
☐ Technical Vulnerability (complete 4b)	☐ Root Compromise
☐ Equipment Missing or Lost (complete 4c)	☐ Web Site Defacement
☐ Equipment Stolen or Damaged (complete 4c)	☐ Other (specify)

4a. Provide the name(s) of the virus(es) and any URLs used to obtain information specific to the virus. Provide a synopsis of the incident and any actions taken to disinfect and prevent further infection.

4b. Generally describe the nature and effect of the vulnerability. Describe the conditions under which the vulnerability occurred and the specific impact of the weakness or design deficiency. Has the application vendor been notified?

4c. Provide the make, model, serial number, and tag number:

5. Information on Affected System:

IP Address:	Computer/Host Name:	OS (include release number):	Other Applications:

6. Information on Affected Hardware/Software:

(include version and release information)

7. Number of Host(s) Affected:

☐ < 10 ☐ 10 to 50 ☐ 50 to 100 ☐ > 100

8. IP Address of Apparent or Suspected Source:

Source IP Address:	Other information available:

9. Incident Assessment:

Is this incident a threat to life, limb, or a critical agency service? ☐ Yes ☐ No If yes, elaborate:

List the most restricted classification of the data residing on the system.

Damage or observations resulting from the incident:

10. Information Sharing:

Who can this information be shared with, outside the Office of the CIO? (do not leave blank and check all that apply)

☐ Other Agencies ☐ Law Enforcement ☒ US-CERT ☐ **No sharing is Authorized**

11. Additional Information:

If this incident is related to a previously reported incident, include previous incident information

Return this form to: State Information Security Officer, 501 S. 14th Street, Lincoln, NE