APPENDIX H: WNC DOCUMENTATION DATA LIST

The following table lists data that should be documented for an incident.

Information to Record	Description
Work Order Number	Use the assigned Help Desk ticket number
Severity Level	Class 1, 2, 3
Type of Incident	Note all types that apply: 1. Reported Vulnerability 2. Compromised System 3. Compromised User Credentials 4. Lost Equipment / Theft 5. Unauthorized Disclosure 6. Physical Break-In 7. Policy Violation 8. Law Enforcement / Legal Hold Request
Incident Timeline	Date/time that the incident was discovered Date/time that the incident was reported Date/time that the incident occurred (if known) Date/time that the incident was closed
Who or what reported the event	Contact Information for reporting party: Full name, organization unit/ department, email address, phone number, location (mailing address, office room number. If an automated system reported the event include the name of the reporting system, the physical location, hostname, network address.
Incident Contact Information	List contact information for all parties involved in the incident resolution
Detailed Description of the event	Include as much information as possible such as: Description of the incident (how it was detected, what occurred) Description of the affected resources Description of the affected organizations Estimated technical impact (i.e. data deleted, system crashed, app available) Summary of response actions performed Cause of the incident List of evidence gathered Total hour spent on the incident (estimate) Incident Handler Comments
Sensitivity of Data	Determine the classification of the incident based on the standards in this document and note if personally identifiable information is involved.
Identification of the host(s)	Source of the Incident: List of source host name, IP address Target of the Attack: Host name/ IP Address (**Target of the attack should not be listed for incidents involving protected health information, NRS protected PII, or sensitive student information**)
Incident Handling Action Log	Include: actions taken, when, by whom. Be detailed, including commands issued, file names, conversations, e-mail's, date and times
Physical Security controls	If there is limited physical access to the computer, document the physical security controls that limit access (ask the person reporting the incident to describe what they have to do to access the computer).
Status of Incident	Open, Ongoing Investigation, Closed