

LINCOLN COUNTY SCHOOL DISTRICT

SECURITY INCIDENT REPORT

Form GBB22-F2 / Regulation GBB22-AR, Section 5, Information Technology

REPORT IMMEDIATELY — and in no case later than the end of the next business day. Do not attempt to remediate, reinstall, delete or “clean up” anything. Preserve the affected device and account exactly as they are. Prompt, good-faith reporting will not be a basis for discipline. If the incident is in progress, telephone the Technology Department first and submit this form afterward.

SECTION 1. REPORTING EMPLOYEE

Name: _____ Position: _____
School/Department: _____ Supervisor: _____
Telephone: _____ Email: _____
Date/time this report submitted: _____

SECTION 2. INCIDENT TIMING

Date/time incident discovered: _____
Date/time incident occurred, if known: _____
Location (site, room, or remote): _____

SECTION 3. TYPE OF INCIDENT

Check all that apply:

- ☐ Lost or stolen District device
- ☐ Lost or stolen personally owned device containing District data
- ☐ Compromised, shared or exposed password
- ☐ Phishing email — opened only
- ☐ Phishing email — clicked a link or opened an attachment
- ☐ Phishing email — entered credentials or other information
- ☐ Ransomware, extortion or lock-screen message
- ☐ Malware or antivirus alert
- ☐ Unauthorized access to an account, system or physical space
- ☐ Unauthorized or accidental disclosure of data (including a misdirected email)
- ☐ Lost, unsecured or improperly discarded paper records
- ☐ Lost or unencrypted removable media

☐ Unexplained system or account behavior

☐ Other: _____

SECTION 4. WHAT HAPPENED

Describe the incident in your own words. Include what you clicked, opened, entered or sent; what you saw; and anything unusual that preceded it. Attach a screenshot or the original message if you have one. Do not delete the message.

SECTION 5. SYSTEMS, DEVICES AND ACCOUNTS AFFECTED

District username(s): _____

Device type and asset tag: _____

Systems or applications involved: _____

Was the device connected to the District network at the time? ☐ Yes ☐ No ☐ Unknown

Is the device still in your possession? ☐ Yes ☐ No

SECTION 6. INFORMATION POTENTIALLY INVOLVED

This section determines whether an evaluation under NRS 603A.220 is required. If you are unsure, check "Unknown" rather than guessing.

☐ Pupil records or pupil personally identifiable information

☐ Employee personnel or payroll information

☐ Social Security numbers or government identification numbers

☐ Financial account or payment card information

☐ Health information

☐ Other confidential District information: _____

☐ No confidential information involved

☐ Unknown

Approximate number of individuals whose information may be involved: _____

SECTION 7. ACTIONS ALREADY TAKEN

Check only what you have actually done. Do not take further action unless directed by the Technology Department.

☐ Disconnected the device from the network (unplugged cable or turned off Wi-Fi)

☐ Left the device powered on and untouched

☐ Powered the device off

☐ Changed my password

☐ Notified my supervisor

☐ Telephoned the Technology Department

☐ Notified law enforcement

☐ Other: _____

☐ No action taken

Others who witnessed or were notified: _____

Reporting employee signature: _____

Date: _____

FOR TECHNOLOGY DEPARTMENT USE ONLY

Received by: _____ Date/time: _____

Ticket/incident number: _____ Severity: ☐ Low ☐ Moderate ☐ High

Containment actions taken:

Superintendent or designee notified: ☐ Yes ☐ No Date/time: _____

Personal information as defined in NRS 603A.040 potentially acquired by an unauthorized person:

☐ Yes ☐ No ☐ Under review

Evaluation under NRS 603A.220 required: ☐ Yes ☐ No

If yes, referred to Superintendent and legal counsel on: _____

Referral to law enforcement: ☐ Yes ☐ No Agency: _____

Records preservation confirmed with business office before any wipe, reset or reimage:

☐ Yes ☐ Not applicable

Resolution summary:

Date closed: _____

Closed by: _____