The purpose of this document is to plan, prepare and execute in the event of a Ransomware attack on Community School District 200's network.

Planning Phase

1. Security awareness and future risk analysis.
    a. Establish two factor authentication (2FA) for the following programs
        i. iVisions
        ii. Synergy
        iii. Gmail (once per device)
    b. Communicate with critical 3rd party applications about the possibility of using 2FA
    c. Phishing & Ransomware campaign
        i. 1 training yearly
        ii. Quarterly campaign information
    d. Ensure backups are running correctly and are succeeding daily.
    e. Ensure Sentinel One is installed on all endpoint devices including windows machines, macs and servers.
    f. Ensure Windows updates are being done on a regular schedule.
    g. Ensure VMware updates are monitored and installed on a regular basis.
    h. Ensure hardware and software updates are being installed on our server infrastructure.
    i. Create an incident response team.
    j. Find a 3rd party vendor to help with detection and removal
        i. Sentinel One for day-to-day operations
        ii. CLIC recommended partner if escalation is required.
    k. Store all necessary contact and service contracts offline.
        i. Cell phone numbers of those that need to know what's going on
        ii. This procedure should be offline
        iii. Phone numbers of necessary vendors needed.
    l. Identify data priority.
        i. Data: payroll information, financial records, facilities records, IEP information, general student records
        ii. Services: iVisions, Synergy, Google

2. Prepare for the attack.

    a. Backups are currently housed at four locations: on local disk, in the cloud, usb disks at Hubble and then monthly sent to Johnson on tape.
        i. Sean will configure alerts to let the response team know that backups are running properly on a daily basis.
        ii. BJ will teach the response team how to create the monthly backups that go off site on tape.

iii. Sean will teach the response team how to get the backups off of the cloud.
iv. The local disk backups are nightly of all our data, weekly backups to USB drives are of all our data, monthly tapes to Johnson are of all our data and cloud backups which happen multiple times a day are of only our critical systems.

Response Phase

3. Execution steps for a Ransomware attack.
    a. Verify the attack is real.
    b. Notify the incident response team.
        i. If the phones are down contact them through email, text or cell
            1. Incident Response team phone numbers needed here. Both cell and desk phone.

Person	[redacted]
BJ Gray	
Len Bonk	
Daniel Sage	
Laura Morris	
Jason Spencer	
David Maksymiw	
Tim Ward	
Lesley Boyum	
Brian O'Keeffe	
Erica Loiacono	
Jeff Schuler	

    c. Determine which systems were impacted and isolate them immediately. In the event you can not disconnect them, power the systems off to ensure the spread does not continue.
        i. All Server infrastructure infected will be done by the network team:
            1. BJ Gray
            2. Daniel Sage

3. Len Bonk
4. Sean Figg

ii. All other endpoints infected will be removed from the network by the helpdesk team directed by Tim and Dave.

d. Perform a thorough investigation.
   i. Identify the extent of the breach.
   ii. Call in the third party vendor if needed to investigate and remove malicious infection.
   iii. Call insurance company
      1. CLIC contact number:
   iv. Contact the local FBI office to inform them of the breach.

e. Eradicate malware and recover.
   i. Eliminate the threat completely
   ii. Start restoring critical applications first
      1. List of critical application here

Synergy Production and Web servers Infinite Visions Servers (APP and DB) WinSnap (vmwinsnapser) FTP Data Transfer server (10.100.20.55) Phone System

   iii. Restore everything else

Prevention Phase

a. Perform post-incident activities
   iv. Regulatory and breach notification requirements
      1. List what and who needs to be contacted to inform them of a breach.
   v. Verify restores of all applications are accounted for.

b. Perform analysis and learn from the attack.
   vi. Discover and analyze why the attack occurred.
   vii. Apply appropriate actions to remove the vulnerability.
   viii. Analyze how the ransomware incident response plan performed.
   ix. Review the ransomware incident response plan and update it as needed.