ACCESS District Network Intrusion Response Plan

Preventative Measures

ACCESS

- ACCESS will apply ALL security patches to all ACCESS severs when they become available
- ACCESS will provide security applications to protect network infrastructure and systems.
- ACCESS will monitor CERT and Microsoft advisories for potential new threats
    - ACCESS will notify districts of these potential new threats
    - ACCESS will take proactive action to minimize the threat when possible
- ACCESS will monitor network backbone usage and intra-district fiber link usage via PRTG Network Monitoring application
    - PRTG will notify ACCESS if any link exceeds the established usage threshold
- ACCESS will develop a system to help district technology coordinators provide meaningful workstation names on all district Windows computers
    - Workstation names are critical to finding infected systems on a district network
- ACCESS will collect and mange a network emergency call distribution list
    - Districts will provide phone numbers and fax numbers for network emergency notification
    - ACCESS will install an automated telephone/fax notification system
- ACCESS will maintain adequate resources to provide district treasurers with an alternate site for payroll and accounting processing

DISTRICT

- Districts will provide professional development sessions for all district personnel on secure computing practices
    - Not opening e-mail attachments from unknown or suspicious senders
    - Applying security patches when necessary
    - Notebook computer security
- Districts will require any user connecting to the ACCESS network from outside of the network to have current virus protection in place, including notebooks, home computers connecting through VPN or dial-up
- Districts will verify a vendor or other non-employee has updated virus detection software on any computer they wish to connect to the network for demonstrations or presentations

- District will keep an up to date inventory of all computers, including specialized computers used for HVAC control, Security, Telephones, Bell Systems, etc

Reactive Measures (an intrusion has been detected)

- ACCESS will immediately secure the backbone and the mission critical servers
    - This will include securing the fiber network electronics at the district level if necessary
- ACCESS will implement the emergency notification system
    - Information regarding the intrusion and what needs to be done will be sent to each district contact on the emergency list
    - ACCESS web page will be updated with information on worm containment and removal
- ACCESS will provide information to help districts identify, quarantine and remove the intrusions
- ACCESS will monitor and if necessary shutdown the link to a district that presents a real threat to the security of the ACCESS network until the treat is removed

Emergency District Clean-up

- A district that faces a large virus cleanup, can request assistance from ACCESS and the two county ESCs
    - The ESCs will maintain a list of technicians willing to work as part of a cleanup team after school hours and on the weekends
    - The district will be responsible for costs incurred by the ESCs for the cleanup
    - ACCESS will work with the cleanup teams to determine what needs to be done and then verify the problem has been resolved