Preventative Measures Checklist

- Ensure domain controllers cannot communicate outbound to the internet.

- Ensure backup systems are not accessible via the internet or from school / office workstations.

- If offline/offsite backups do not exist, copy all current backups to external media (in a repeatable process).

- Do not allow RDP (Remote Desktop Protocol – TCP port 3389), SSH (Secure Shell – TCP port 22), and File Shares (SMB – TCP port 445) to be accessible from the Internet. These protocols are commonly used as an initial attack vector. These services should only be available to remote users and external partners through the use of a Virtual Private Network) VPN. If a service or protocol is not needed it should be disabled.

- Audit any new accounts added in Active Directory over the past 30 days.

- Adhere to the principal of least privilege, ensuring that users have the minimum level of access required to accomplish their duties. Remove local administrator access for everyone except for designated administrator.

- Increase employee awareness on identifying suspicious emails containing URLs/attachments and that any such emails should be reported to the IT department immediately.

- Patch all systems with latest stable patches available.

- Use web filtering where possible to block access to malicious and “unknown” websites.