Cyber Defense Checklist

What can schools do to improve their defense against cyberattacks? The following checklist will aid in identifying potential vulnerabilities and areas where action should be taken.

1. Do you use multi-factor authentication on all remote access; staff email; privileged accounts; secure backups and BOCES service ? Yes☐ No☐

2. Does every device in your organization have End Point (anti-virus) and Malware software installed? Yes☐ No☐

3. Is the End Point and Malware software up to date? Yes☐ No☐

4. Have you installed all relevant security patches on every system in your environment, e.g., desktops, laptops, mobile devices, servers, firewalls, routers, switches? Yes☐ No☐

5. Do any third parties have access to your network? Yes☐ No☐

6. What systems can they access? _____

7. Did you use NYSIR's Data Services Insurance Specifications in your contracts with third parties that can access your network? Yes☐ No☐

8. Is multi-factor authentication required of third parties when connecting to your network? Yes☐ No☐

9. Do you review the security controls of third parties to ensure they meet the requirements of Education Law 2-d and have adequate controls in place to protect your data? Yes☐ No☐

10. Do you have firewalls in place between your networks and the internet? Yes☐ No☐

11. Do you limit incoming country IP addresses to the United States and Canada? Yes☐ No☐

12. Do you encrypt all mobile devices (Chromebooks, laptops, phones, tablets, USB sticks)? Yes☐ No☐

13. Do you encrypt and limit all sensitive/confidential network data both at rest and in transit? Yes☐ No☐

14. Do you require the use of strong passwords? Yes☐ No☐

15. Do you require passwords be changed at least every 60 days and have anti-repeat and common-word restrictions? Yes☐ No☐

16. Do you use email filtering? Yes☐ No☐

17. If yes, what email filtering system is used? _____

18. Have you used the NYSIR PII Self-Assessment Tool to assess your PII vulnerability? Yes☐ No☐

19. Is PII data at rest and in transit encrypted? Yes☐ No☐

20. Does the District's/BOCES' data retention policy comply with NYSED Ed Law 2-d? Yes☐ No☐

21. Do you regularly purge data that is outside your stated retention periods? Yes☐ No☐

22. Do you perform regular backups of all critical systems? Yes☐ No☐

23. Are your backups stored in a secure off-site location that won't be impacted by a malware or ransomware event? Yes☐ No☐

24. Are backups stored on a separate server not connected to the internet? Yes☐ No☐

25. Have you tested your backup data to ensure it will work should you have to clear all devices and reinstall? Yes☐ No☐

26. Do you provide cyber-security awareness training (phishing, password security, social engineering) for all employees annually? Yes☐ No☐

27. Do you limit administrative privileges to only those individuals who require access in order to perform their job functions? Yes☐ No☐

28. Have you implemented the principle of least privilege to allow employees to access only the data they need to perform their job functions? Yes☐ No☐

29. Do you keep an inventory of all devices, applications, software and hardware on your network, and ensure its updated frequently? Yes☐ No☐

30. Have you implemented a formal change-management process for all critical systems? Yes☐ No☐

31. Do you have any Legacy hardware or software? Yes☐ No☐

32. Are vulnerability tests performed? Yes☐ No☐

33. Have penetration tests been performed? Yes☐ No☐

34. How many "Yes" responses did you record?

- 26 Excellent! Keep up the terrific work.
- 23 to 26 Good start! Keep going.
- < 22 You have vulnerabilities! Keep making improvements.