

JPA Risk Management 2026-2027 Cyber Questionnaire

As you are aware, cyber security and, specifically, multi-factor authentication (MFA) and software vulnerabilities have been identified as top areas of concern. Additional cyber security questions are listed below. A response to these questions is required of all JPA members.

If previously completed, please only address any changes or updates on line 16. Please submit your answers no later than 01/31/26.

We appreciate your time in responding to this survey! If you have any questions, please feel free to contact Julie Nester at julie.nester@sdcoe.net or 858-295-6956 to discuss. You can also contact SDCOE IT for general information and questions at securinginfo@sdcoe.net, via telephone at 858-298-2211, or by visiting their website at cybersecurity.sdcoe.net.

*Required

1. JPA Member Organization*

2. Name*

3. Email Address*

4. Phone Number*

5. Are critical software patches implemented within 30 days? *

6. Is there a Privileged Access Management (PAM) tool deployed? *

7. Is all data "at rest" and "in transit" encrypted? *

8. Are all mobile computing devices encrypted and do they have endpoint protection implemented? *

9. Does your district/school have any software or hardware that is no longer supported or has been identified as end-of-support by the software or hardware vendor that is still being used within their network? *

10. How often are phishing simulations conducted? *

11. How many sensitive records (SSNs, Financial Information, etc.) are held or processed through the network? *

12. Does your district/school have a formal cyber incident response plan and is it tested periodically? *

13. Has Multi Factor Authentication (MFA) for remote access to network and email been implemented? *

14. Are formal back-up procedures in place that are tested minimally on an annual basis? *

15. Is there an Endpoint Detection & Response (EDR) solution deployed to all endpoints? *

16. Please address any changes or updates: *

☐ No changes

☐ Other: