CHOOSING THE RIGHT MSP

1. IDENTIFY YOUR SCHOOL'S SPECIFIC SECURITY NEEDS

- Assess current cybersecurity risks and vulnerabilities.
- Determine the specific security services required (*e.g., threat detection, incident response, compliance management*).

2. EXPERIENCE AND EXPERTISE IN THE EDUCATION SECTOR

- Verify the MSP's experience in working with educational institutions.
- Check for a prom track record in handling the unique security challenges faced by schools.

3. COMPREHENSIVE SECURITY SERVICES

- Ensure the MSP offers a full suite of security services, including: *network security, endpoint security, cloud security, data protection, and compliance management.*

4. PROACTIVE THREAT MONITORING AND RESPONSE

- Confirm the MSP provides 24/7 threat monitoring and quick incident response.
- Look for advanced threat detection technologies and proactive measures to prevent attacks.

inspiroz
an ACS Company

CHOOSING THE RIGHT MSP

5. STRONG DATA PROTECTION AND PRIVACY MEASURES

- Assess the MSP's policies on data protection and privacy.
- Ensure they comply with relevant regulations, such as FERPA and GDPR.

6. CUSTOMIZED SECURITY SOLUTIONS

- Determine if the MSP can tailor their services to meet your school's specific needs.
- Check for flexibility in scaling services as your school's requirements evolve.

7. TRANSPARENT PRICING AND CONTRACT TERMS

- Review the MSP's pricing structure to ensure it aligns with your budget. Avoid long-term contracts without performance evaluation clauses..

8. REPUTATION AND REFERENCES

- Research the MSP's reputation within the industry.
- Request references from other educational institutions they have served.

CHOOSING THE RIGHT MSP

9. CERTIFICATION AND COMPLIANCE

- Verify the MSP's certifications (e.g., ISO 27001, SOC 2).
- Ensure they adhere to industry standards and best practices.

10. INCIDENT RESPONSE AND RECOVERY PLANS

- Evaluate the MSP's incident response strategies and recovery plans.
- Ensure they have robust protocols for minimizing downtime and data loss during security incidents

11. ONGOING SUPPORT AND TRAINING

- Confirm the availability of continuous support and regular security updates.
- Ensure the MSP offers training for your staff on cybersecurity best practices.

12. TECHNOLOGY AND TOOLS

- Assess the MSP's use of the latest security technologies and tools.
- Ensure they leverage AI and machine learning for e detection.

inspiroz
an ACS Company