Resources on Understanding the Role of Information Technology Specialists in Supporting School Safety Before, During, and After an Emergency

Cybersecurity and Cyber Safety Considerations for Schools and Districts

Cybersecurity Considerations for K-12 Schools and School Districts (REMS TA Center). Access this online course from the REMS TA Center on the topic of cybersecurity in the school setting. https://rems.ed.gov/trainings/CourseCybersecurity.aspx

Cybersecurity Considerations for K-12 Schools and School Districts (REMS TA Center). Read about cybersecurity considerations for K-12 schools in this fact sheet. https://rems.ed.gov/docs/Cybersecurity_K-12_Fact_Sheet_508C.PDF

Cyber Safety Considerations for K-12 Schools and School Districts (REMS TA Center). Review this fact sheet to learn about how schools and school districts can prepare for human-caused cyber threats, such as incidents that can disrupt education and critical operations; expose personally identifiable information of students, teachers, and staff; and lead to high recovery costs. https://rems.ed.gov/docs/Cyber_Safety_K-12_Fact_Sheet_508C.PDF

Getting Smarter About K-12 Cybersecurity (U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency). Access this Webinar to learn more about how schools and school districts can protect their systems from cyberattacks and threats. https://www.youtube.com/watch?v=ESbP0YmsTrw
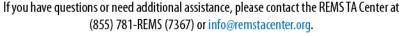
Dear School Safety Partner: Cybersecurity and Cyber Safety (REMS TA Center). Learn more about cybersecurity and cyber safety with this TA Snapshot featuring information on various threats facing school district networks and systems and a selection of related resources. https://rems.ed.gov/docs/TASnapshot_CybersecurityCyberSafety_508C.pdf

Guide for Cybersecurity Event Recovery (U.S. Department of Commerce, National Institute of Standards and Technology). Review this guide to learn about how to improve resilience and plan for recovery against cybersecurity threats. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS REMS TECHNICAL ASSISTANCE CENTER

If you have questions or need additional assistance, please contact the REMS TA Center at (855) 781-REMS (7367) or info@remstacenter.org.

@remstacenter   https://rems.ed.gov

K-12 Cybersecurity Self Assessment (EdTech Strategies). Complete this self-assessment for school district information technology (IT) leaders to identify areas for strengthening cybersecurity controls. https://k12cybersecure.com/resources/k-12-cybersecurity-self-assessment/

Protect Your Network: Strengthen Your Cybersecurity With Our Incident Response Training (U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency). Watch this series of Webinars focused on cyber incident response training for government employees and contractors in Federal, state, local, tribal, and territorial agencies. https://www.youtube.com/playlist?list=PL-BF3N9rHBLJaSbTRPyWYj56f0m2uDQD7

Cybersecurity Incident & Vulnerability Response Playbooks (U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency). Use these playbooks to implement a standard set of operational procedures for planning and conducting cybersecurity vulnerability and incident response activities. https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

Cyber Essentials Starter Kit: The Basics for Building a Culture of Cyber Readiness (U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency). Use this guide to understand the basics for building a culture of cyber readiness, and develop an actionable understanding of where to start implementing organizational cybersecurity practices.
https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Starter%20Kit_03.12.2021_508_0.pdf

Cybersecurity and Cyber Safety Considerations for Students and Staff

Protecting Kids Online (U.S. Federal Trade Commission). Access this Web page for resources on talking to kids about cybersecurity and cyber safety. https://consumer.ftc.gov/identity-theft-and-online-security/protecting-kids-online
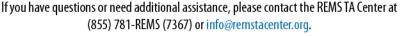
Cyber Security and Protecting Students and Staff (REMS TA Center). Join this virtual Community of Practice forum to discuss cybersecurity and protecting students and staff data. https://rems.ed.gov/COP/REMSCOPforum/topics.aspx?ForumID=138

Cyber Safety Quick Links for Protecting Youth: Empowering Students to Become Responsible Digital Citizens and Engage Online Safely (REMS TA Center). Access this TA Snapshot for an overview of cyber safety and key practical and quick links to Websites offering free cyber safety resources, tools, and training for youth, parents, and school personnel. https://rems.ed.gov/docs/CyberSafetyProtectingYouth_COVID19_508C.pdf

READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS **REMS** TECHNICAL ASSISTANCE CENTER

If you have questions or need additional assistance, please contact the REMS TA Center at (855) 781-REMS (7367) or info@remstacenter.org.

@remstacenter   https://rems.ed.gov

Keeping Your Child Safe Learning Online: Understanding Student Data Privacy (U.S. Department of Education, Office of Educational Technology). Read this article to find out more about maintaining student safety and data privacy when using educational technology. https://medium.com/keep-calm-and-connect-all-students/keeping-your-child-safe-learning-online-f47811a1784d

Cybersecurity in the Classroom (U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency). Visit this Web page to access K-12 cybersecurity curricula and education tools. https://niccs.cisa.gov/formal-education/integrating-cybersecurity-classroom

Information Technology Infrastructure
Tools

Building Technology Infrastructure for Learning (U.S. Department of Education, Office of Educational Technology). Use this K-12 school infrastructure guide to navigate the many decisions required to build a technology infrastructure that supports digital learning. https://tech.ed.gov/infrastructure/

Data Security Checklist (U.S. Department of Education, Privacy Technical Assistance Center). Use this checklist to develop, maintain, and improve your data security program. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Data%20Security%20Checklist.pdf
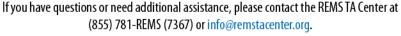
Cybersecurity Framework (U.S. Department of Commerce, National Institute of Standards and Technology). Visit this Web page to better understand the National Institute of Standards and Technology cybersecurity framework and cybersecurity supply chain risk management. https://www.nist.gov/cyberframework

Cyber Essentials Toolkits (U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency). Access this online set of learning modules that breaks down the Cybersecurity and Infrastructure Security Agency (CISA) Cyber Essentials into bite-sized actions for IT and C-suite leadership to follow and fully implement each Cyber Essential. https://www.cisa.gov/publication/cyber-essentials-toolkits

Nationwide Cybersecurity Review (Center for Internet Security, Multi-State Information Sharing and Analysis Center). Complete this no-cost, anonymous, annual self-assessment to receive organization-specific metrics to identify gaps in your current cybersecurity capabilities, develop a benchmark to gauge progress, and gain access to a repository of informative resources. https://www.cisecurity.org/ms-isac/services/ncsr

Data Breaches

Stop Ransomware: K-12 Resources (U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency). Visit this Web page for your education staff to obtain resources related to cybersecurity best practices as well as cyber threats such as ransomware. https://www.cisa.gov/stopransomware/k-12-resources

K-12 Education Leaders' Guide to Ransomware: Prevention, Response, and Recovery (U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency). Watch this informational Webinar to learn about strategies schools can take to prevent, respond to, and recover from ransomware attacks. https://www.youtube.com/watch?v=h0J7qGSOVa4

Ransomware Reference Materials for Parents, Teachers and School Administrators (U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency). Access this Web page to find resources for school staff, caregivers, and families on cyber threats such as ransomware, phishing, and malware. https://www.cisa.gov/stopransomware/ransomware-reference-materials-parents-teachers-and-school-administrators

Ransomware Reference Materials for K-12 School and School District IT Staff (U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency). Visit this Web page to access resources for school and school district staff, including IT staff, on cyber threats facing K-12 schools. https://www.cisa.gov/stopransomware/ransomware-reference-materials-k-12-school-and-school-district-it-staff

Data Breach Scenario Trainings (U.S. Department of Education, Privacy Technical Assistance Center). Participate in these professional learning opportunities to learn more about data breaches in school settings. https://studentprivacy.ed.gov/resources/data-breach-scenario-trainings

Dual Enrollment Data Breach Scenario (U.S. Department of Education, Privacy Technical Assistance Center). Engage in this specialized tabletop exercise to learn about dual enrollment data breaches and develop a response plan to address a potential data breach. https://studentprivacy.ed.gov/resources/dual-enrollment-data-breach-scenario
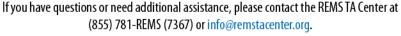
Emergency Operations Plan (EOP) Development and Annexes

Creating, Revising, and Enhancing Emergency Operations Plans to Support Cyber Safety (REMS TA Center). Access this two-part podcast from the REMS TA Center on the topic of cyber safety in the school setting. https://rems.ed.gov/podcast

Integrating Cybersecurity With Emergency Operations Plans (EOPs) for K-12 Schools (REMS TA Center). Watch this Webinar to learn about the importance of cybersecurity and network protection at schools and school districts. Presenters represent the U.S. Department of

Education and the U.S. Department of Homeland Security's Office of Cybersecurity and Communications. https://rems.ed.gov/webinarDetail?id=34

Guide for Developing High-Quality School Emergency Operations Plans (School Guide) (U.S. Department of Education, U.S. Department of Health and Human Services, U.S. Department of Homeland Security, U.S. Department of Justice, Federal Bureau of Investigation, and Federal Emergency Management Agency). Read about the six-step planning process for schools to develop, revise, or review a school EOP. https://rems.ed.gov/docs/REMS_K-12_Guide_508.pdf

The Role of Districts in Developing High-Quality School Emergency Operations Plans (District Guide) (U.S. Department of Education, U.S. Department of Justice, U.S. Department of Health and Human Services, and U.S. Department of Homeland Security). Read about how school districts can fulfill both their individual and their shared emergency planning responsibilities in school EOP development. https://rems.ed.gov/docs/District_Guide_508C.pdf

Using a Six-Step Planning Process and Scenario-Based Planning to Support Emergency Operations Plan Development Web Page (REMS TA Center). Access resources from the REMS TA Center, the U.S. Department of Education, and Federal agency partners on the topic of EOP development. https://rems.ed.gov/Resource_Plan_Basic_EOP.aspx

READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS **REMS** TECHNICAL ASSISTANCE CENTER

If you have questions or need additional assistance, please contact the REMS TA Center at (855) 781-REMS (7367) or info@remstacenter.org.

@remstacenter   https://rems.ed.gov