LOUISIANA DEPARTMENT OF EDUCATION

Educational Technology Monthly Call

May 2022

https://bit.ly/EdTech-May2022

Agenda

- Education Technology Updates
- Cybersecurity
- Emergency Connectivity Fund, E-Rate, and ACP
- Important Reminders and Other Information

Suggested participants
for this call:

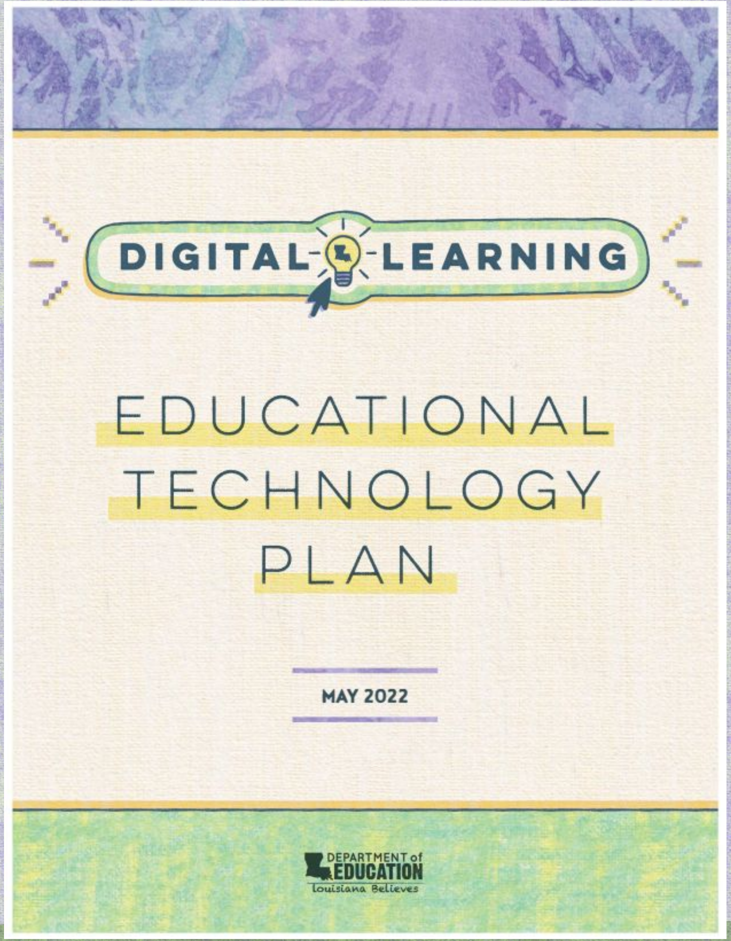
- Chief Technology Officers
- Information Technology Staff
- E-Rate Coordinators
- Privacy Coordinators
- Digital or Virtual Learning Staff

Education Technology Updates

EdTech Plan

- **It's live!**
  - Digital Learning website

- This revised educational technology plan is **intended to be a guide** to inform and influence school systems in crafting their own strategic technology plan. This plan also serves as a guide for school leaders in **developing a framework for educational technology integration** at the school level.



DIGITAL LEARNING

EDUCATIONAL TECHNOLOGY PLAN

MAY 2022

DEPARTMENT of EDUCATION
Louisiana Believes

5 Strategic Goals

- Prepare teachers and educational leaders to **effectively integrate technology** into high-quality teaching and learning environments.
- Create and nurture **equitable access to high-quality, inclusive learning environments** for parents and learners of all ages.
- Cultivate high-impact systems, structures, and partnerships to provide access and foster continuous learning including facilitating **broadband Internet access in every student and educator's home in Louisiana.**
- Provide high-quality teaching and learning environments by **ensuring continued availability of effective digital technology** for every student, teacher, educational leader, and classroom in Louisiana.
- Implement programs that **facilitate technology fluency** so all students are on track to a professional career, college degree, or service.

Why is this important?

- The effective use of educational technology is essential in the 21st century classroom. The pandemic was a catalyst for exponential growth in edtech and it is our responsibility to harness that potential and guide it to facilitate growth for our students, teachers, and school systems.

- Educational technology integration was not a temporary adjustment as a response to the pandemic, but a permanent element in education and collective guidance is essential to state-wide success.

What will success of this plan look like?

We can gauge the success of this plan through transparency, accessibility, and alignment with academic goals.

- **Transparency**
  - Students and staff are equipped with the knowledge to seamlessly integrate technology into instruction without compromising academic success.

- **Accessibility**
  - Technology is readily available to all students and teachers across the state evenly

- **Academic alignment**
  - Meaningful integration that expands learning and creates new opportunities unavailable before aligned with the department's academic goals

What do we need in the future?

- It is essential that we ensure access and connectivity to all students and teachers across the state and couple this with analysis on relevant instructional technology tools and best practices to create a successful learning environment for all students.

- Moving forward, we have to be vigilant in evaluating our technology processes and applications. New technologies are ever-emerging and it is our responsibility to continue to adapt to this evolving horizon.

Technology Readiness Tool (TRT) Data Collection

- A session on TRT will be held at LaCUE's Technology Leadership Summit.
- School systems should plan on documenting both devices, network, broadband access and security for the Fall 2022 TRT Data Collection.
- The collection requires schools to submit data on the following:
  - Devices used by students and teachers including
  - School-level and/or District-level network infrastructure
  - School-level and/or District-level internet access speeds
  - Student off-campus/home broadband access
  - School Information/Network Security
- Data submission window will open in September and be due by the end of October.
- All public schools, charter schools, and scholarship schools must submit data per State law.
- Non-scholarship non-public schools are encouraged to at least submit school information/network security data which will be used to support and guide future cybersecurity efforts.

Reminder: Change in Education Technology Monthly Webinar and Office Hours

Office hours for May and June will be cancelled along with the monthly calls for June and July. We will however hold an office hour call in July ahead of the start of school to prepare for the upcoming school year. Additionally we will be at the LaCUE Technology Leadership Summit in June.

Dates	• May 26, 2022 9:00 AM - Monthly Webinar • June 9, 2022 9:00 AM - Office Hours - CANCELLED • June 23, 2022 9:00 AM - Monthly Webinar - CANCELLED • July 28, 2022 @ 9:00 AM - Office Hours

In SY 22-23, we swap around dates and start holding the Monthly Webinar on the 2nd Thursday of the month and holding the Office hours two weeks later. See Dates in the Reminders section.

Registration for the Technology Leadership Summit is OPEN!

Registration for the 2022 Technology Leadership Summit is now OPEN! #TLS22 will be held from **June 13-15, 2022** at the Marriott Hotel in Baton Rouge, Louisiana.

Keynote speaker: Dr. Joe Sanfelippo, author of Lead from *Where You Are* and *Hacking Leadership*.

Regular registration amount of $150. Go to members.lacue.org to register.

LACUE Technology Leadership Summit Pre-Conference:

Pre-Conference Registration: https://bit.ly/TLS22Pre-Con (this is a separate registration)

All pre-conference attendees must be registered for Summit to participate in the tabletop exercise.

LACUE Technology Leadership Summit
Pre-Conference:

Cybersecurity Tabletop Exercise (12:30-3:30)

Target Audience: District IT teams responsible for supporting the district’s network and a response in the event of a cyber-incident.

Pre-Conference Registration Required: Note that this is a separate registration in addition to the main Summit Registration which is required to participate.

The cybersecurity tabletop exercise will simulate an actual cybersecurity crisis. Your district’s IT Team will be presented with several scenarios where members will discuss their roles and their responses to the particular situation. Time will be provided after each of the 3 modules to share with all districts in attendance. Representatives from the Cybersecurity and Infrastructure Security Agency (CISA) and GOHSEP will serve as facilitators to present the scenarios and to guide discussion.

LACUE Technology Leadership Summit Pre-Conference:

ExtremeCloud IQ Makes Wi-Fi Simple (12:00 – 4:30)

Target Audience: District IT teams.

Pre-Conference Registration Required: There is no charge for this event; however, all attendees for this pre-conference must be registered for the full Summit.

Wouldn’t it be nice if you could onboard, manage, and troubleshoot your wired and wireless network from an app on your phone? What if we could use Artificial Intelligence to solve real problems on the Wi-Fi without requiring a PhD to decipher? In this workshop we will provide hands-on technical training on how to create and deploy ExtremeCloud IQ. Come learn how Extreme Networks is innovating new ways to make networking easy in a world of higher than ever demand.

Cybersecurity

Cyber Advisories & Alerts

Below are the Cyber Advisories and Alerts released by MS-ISAC for May, 2022. The latest advisories and alerts are also available on the Center for Insernet Security (CIS) website here.

- MS-ISAC Advisory # 2022-073: Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution
- MS-ISAC Advisory # 2022-072: Multiple Vulnerabilities in Firefox Products Could Allow for Arbitrary Code Execution
- **MS-ISAC Advisory # 2022-071**: A Vulnerability in VMware Products Could Allow for Authentication Bypass
- MS-ISAC Advisory # 2022-070: Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution
- MS-ISAC Advisory # 2022-069: Multiple Vulnerabilities in SonicWall SSL VPN SMA1000 Series Could Allow for Authentication Bypass
- **MS-ISAC Advisory # 2022-068**: A vulnerability in Zyxel Firewall and VPN Could Allow for Arbitrary Code Execution
- **MS-ISAC Advisory # 2022-067**: A Vulnerability in certain HP PC BIOS Could Allow for Local Arbitrary Code Execution
- MS-ISAC Advisory # 2022-066: Multiple Vulnerabilities in Adobe Products Could Allow for Arbitrary Code Execution

Advisories in **RED - exploit exists in the wild or a proof-of-concept posted

Cyber Advisories & Alerts (Cont.)

- MS-ISAC Advisory # 2022-065: 2022-065: Critical Patches Issued for Microsoft Products, May 10, 2022
- MS-ISAC Advisory # 2022-064: 2022-064: Multiple Vulnerabilities in Google Chrome for Android and Chrome OS Could Allow for Arbitrary Code Execution
- MS-ISAC Advisory # 2022-063: Multiple Vulnerabilities in F5 Networks Products Could Allow for Arbitrary Code Execution
- MS-ISAC Advisory # 2022-062: Multiple Vulnerabilities in Firefox Products Could Allow for Arbitrary Code Execution
- MS-ISAC Advisory # 2022-061: Multiple Vulnerabilities in Firefox Products Could Allow for Arbitrary Code Execution
- MS-ISAC Advisory # 2022-060: Multiple Vulnerabilities in Google Android OS Could Allow for Escalation of Privilege

CISA Cyber Risk Summary - Education Sector

CISA released their annual risk summary of Education entities that participate in their Cyber Hygiene (CyHy) Vulnerability Scanning and Cybersecurity Assessments services. The report ulitized data collected from from October 1, 2020 through September 30, 2021. Outlined below are recommended mitigations to help reduce Cyber Security risk.

- Restrict user network access and access level to the minimum required.
- Enforce MFA authentication and password requirements based on National Institute of Standards and Technology (NIST) best practices.
- Implement network segmentation to separate users from and restrict access to sensitive data. Protect sensitive network segments with firewalls and Intrusion Detection System (IDS) devices.
- Audit and closely monitor account usage and network activity to minimize response time to abnormal activity or network intrusion.
- Configure network firewalls to block unauthorized Internet Protocol (IP) addresses and disable port forwarding.
- Monitor privacy settings and information available on social networking sites.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, secure location.

CISA Cyber Risk Summary - Mitigations

Vulnerability Management:

1. Regularly scanning internet-accessible hosts and remediating critical and high severity vulnerabilities within 15 to 30 days, respectively.
2. Prioritize remediation of vulnerabilities using a risk-based approach that considers likelihood of an attack, the ease of exploitation, and the magnitude of probable impact. It's important to consider remediating active Known Exploited Vulnerabilities (KEVs) first and then defining vulnerability prioritization mechanisms that will consider contextual factors specific to each entity, such as the stakeholder-specific vulnerability categorization (SSVC) framework.

Unsupported Operating System Versions:

1. Entities should identify and plan to allocate resources to replace IT—including software, firmware, OSs, and hardware—that is no longer supported or will reach end of support in the near future.
2. For software or OSs that are unsupported but required to meet business needs, entities should document exceptions and implement mitigating controls such as network segmentation to isolate vulnerable systems.

CISA Cyber Risk Summary - Mitigations

Potentially Risky Services: Certain services such as Network Basic Input/Output System (NetBIOS), Teletype Network (Telnet),Server Message Block (SMB), Remote Desktop Protocol (RDP), and others are vulnerable to being exploited by deployed malware, including ransomware, and facilitate lateral movement throughout a network.

1. All listening network ports and services on a system need a validated business reason to run. Identify all internet accessible services and secure or disable risky services according to the documented business reason for operation of each service.
2. Disabling unused-remote access/RDP ports, monitoring remote access/RDP logs for signs of brute force attacks and other abnormal activity. Ransomware actors frequently abuse RDP via brute force attacks or other vulnerabilities to gain initial access.
3. Require multi factor authentication (MFA) for any remote access service and limit remote user access privileges.
4. Restrict user network access and access level to the minimum required (Least Privilege). Enforce user authentication and password requirements based on NIST-defined best practices.
5. Implement network segmentation to separate users from, and restrict access to, sensitive data. Protect sensitive network segments with firewalls and Intrusion Detection System (IDS) devices.
6. Audit and closely monitor account usage and network activity to minimize response time to abnormal activity or network intrusion.
7. Configure network firewalls to block unauthorized IP addresses and disable port forwarding.

Join The Multi-State Information Sharing and Analysis Center® (MS-ISAC®)

Public K-12 education entities are eligible to join MS-ISAC. Membership is free and joining gives your school access to wide range of benefits and services:

- 24/7 Security Operations Center
- **Cybersecurity Advisories, Alerts, and Newsletter emails**
- Cybersecurity Awareness and Education resources
- Incident response and digital forensics services
- Monitoring of your public IP ranges and domains for possible compromises
- Access to our Malicious Code Analysis Platform (MCAP)
- Weekly top-malicious domains and IPs report
- Cyber Hygiene Services - Vulnerability Scanning, Web Application Scanning, Phishing Campaign Assessment, and Remote Penetration Test
- Block ransomware with Malicious Domain Blocking and Reporting (MDBR) Service
- Access to cyber security tabletop exercises
- CIS SecureSuite Membership including access to CIS Benchmarks, CIS-CAT Pro, CIS WorkBench, remediation content, and more

More information MS-ISAC Services is available here. MS-ISAC membership registration page.

E-Rate,
Affordable Connectivity Program
and
Emergency Connectivity Fund

ECF Update

The Federal Communications Commission (FCC) announced that it received requests for $2,814,736,532 in the third application filing window of the Emergency Connectivity Fund program to fund 5,120,453 connected devices and 4,285,794 broadband connections. Applications will be prioritized to fund schools and libraries with the greatest need first, with a preference for schools and libraries located in rural areas. With approximately $1.5 billion remaining in the program, the FCC expects to be able to fund requests from many of the 7,369 schools and school districts, 628 libraries and library systems, and 133 consortia which applied from across the country.

E-Rate Important Dates and Reminders

- The Form 486 deadline is either 120 days from the FCDL date or the service start date (typically July 1st). Upcoming Form 486 deadlines are:

Wave 42	05/27/2022
Wave 43	06/03/2022
Wave 44	06/10/2022

- **May 16** - FCC comments due on the FCC's Notice of Inquiry regarding the prevention and elimination of digital discrimination (FCC 22-21). Reply comments are due June 30th.
- **May 27** - Reply comments due on the FCC's proposal to create an E-rate competitive bidding portal (FCC 21-124).
- **May 27** - Beginning of the summer deferral period for PIA inquiries
- **May 31** - The extended invoicing deadline for FY 2020 non-recurring services

Reminders and Other Information

2020-2021 Education Technology Webinar and Office Hours

Monthly Call Dates

July - no call
August 11, 2022
September 8, 2022
October 13, 2022
November 17, 2022
December 15, 2022
January 12, 2023
February 9, 2023
March 9, 2023
April 6, 2023
May 11, 2023
June - meet at LaCUE TLS

TIme:	9:00 AM - 10:00 AM
Webinar Link	https://ldoe.zoom.us/j/575223228?pwd=NDNlN01SS3c0Rk4wV25aNkZhTEc2Zz09
Phone Number	1-301-715-8592
Meeting ID	Meeting ID: 575 223 228 Password: 2020-202!

Office Hours Dates

July 28, 2022
August 25, 2022
September 22, 2022
October 27, 2022
Nov - no office hours
Dec - no office hours
January 26, 2023
February 23, 2023
March 23, 2023
April 27, 2023
May - no office hours
June - meet at LaCUE TLS

Thank you for joining today’s call.

Schedules, access links, and information for the Department’s webinars can be found in the LDOE Weekly Newsletter and LDOE School System Support Calendar.

Helpful Links

- A+PEL PD for Educators
- LACUE
- Louisiana Believes Homepage
- School Improvement Library

Support Toolboxes

- Teacher
- System
- Principal
- Counselor
- Education Technology Staff

DEPARTMENT of EDUCATION
Louisiana Believes