VERMONT
AGENCY OF EDUCATION

1 National Life Drive, Davis 5, Montpelier, VT 05620-2501
(p) 802-828-1130 | (f) 802-828-6430 | education.vermont.gov

# 2022 ESSER Cybersecurity Grant Awards

The Agency of Education (AOE) is committed to supporting Vermont supervisory unions and school districts (SU/SDs) in protecting student data and school networks from cyberattacks and exploitation by nefarious individuals. To support Vermont SU/SDs in leading cybersecurity planning efforts for schools within their respective districts, the AOE made available one-time funds for a round of competitive grants to encourage the development of comprehensive data breach response plans and provide assistance in purchasing needed equipment and software to ensure students and educators have continuous network access to the technology needed for instruction. Of particular urgency is cybersecurity planning that protects school network access for activities that address learning loss be it for academic enrichment, extended day, afterschool programs or extended school year programs. Establishing a cybersecurity framework and data breach response plan for a district will help schools better manage and reduce their cyber-security risk and ensure continuous student access to the technology needed to maintain fidelity in instruction. Applicants could apply for grants of up to $30,000. The total amount of funding available for this grant competition was $250,000. This grant program is funded through Elementary and Secondary School Emergency Relief (ESSER) monies under the purview of the Agency of Education. The AOE cyber grant initiative was highlighted in a cybersecurity state spotlight published by the State Educational Technology Directors Association. The topic focus was on incident response planning.

The following SU/SDs are recipients of Cybersecurity Grant Awards: Bennington Rutland SU, Burlington SD, Colchester SD, Essex Westford UUSD, Kingdom East SD, Missisquoi Valley SD, Mt. Mansfield Union SD, Rutland City SD, Two Rivers SU, and Washington Central UUSD.

### Bennington Rutland Supervisory Union: $15,591

Grant funds will be used to purchase network equipment needed to provide a reliable and secure network, either adding or replacing inadequate hardware for best practices. Grant funds also will be used to work with a consultant who is an expert in the NIST framework planning process, to help the district complete the planning process successfully and create a cybersecurity policy that could be approved by the BRSU school boards. Grants funds will be used to address any cybersecurity training needs.

### Burlington School District: $29,820

Funds from this grant will be used to hire a consultant to assist in the creation of new data security and network cybersecurity policies for the district and provide stipends for the anticipated additional after-school time needed by existing staff to complete planning. Grant funds also will be used to provide vulnerability testing services and models and to make any

## Contact Information:

If you have questions about this document or would like additional information, please contact:

Lisa Helme, Student Pathways Division, at lisa.helme@vermont.gov or (802) 828-6956.

needed plan revisions. The grant will cover professional learning memberships and services aimed at securing student data and enhancing the overall security of the district network.

### Colchester School District: $24,475

The grant funds will be used to create a new data security policy and data breach response plan. The purchase of logging, event correlation and response capability, phishing awareness training and multifactor authentication capability will become part of a new cybersecurity policy for the district. Assuming legal consultation may be required in the formal response policy, the district will utilize grant funds to support that.

### Essex Westford Unified Union School District: $30,000

Grant funds will be used to pursue a series of "phishing" exercises to build better awareness amongst district staff on identifying malicious emails and content. This work will better inform the district's efforts around cybersecurity response planning and provide much needed information on the understanding/ability of district staff pertaining to their awareness of cyber-attacks and the means through which attacks are orchestrated. Funds also will used to conduct a 14-day penetration test to better understand the district's network vulnerabilities.

### Kingdom East School District: $29,987

Grant funds will be used for data collection, writing, and collaboration for consultants engaged to work with the team's district personnel and release time (substitutes when needed) for district staff engaged in the Cybersecurity and Data Security Plan writing team. Once the plan is completed, the district will run a tabletop exercise with identified key and representative personnel likely to be targeted to determine workability, effectiveness, completeness, and areas for improvement of the Cybersecurity and Data Breach Response Plan.

### Missisquoi Valley School District: $3,950

Grant funds will enable the district to engage a third party for security consulting. Based on the security company consultant's findings and guidance, a district security policy will be formalized. The security company will provide general security guidance, network assessment assistance, penetration testing, and email phishing campaigns. Much of the work that will be done falls under the identify function in the NIST Framework.

### Mt. Mansfield Union School District: $30,000

The grant funds will provide the district with the tools needed to document network data and workflows and to maintain and monitor logs. The work will help identify threats, vulnerabilities, and the risk to district assets. A large part of the data security planning will be the purchase and implementation of a SIEM - security information and event management system. This system will give the district real-time insight into vulnerabilities, threats, and security events by collecting logs and events from all systems across the district. The SIEM will immediately notify technical staff if there are incidents to respond to. This work will drive the cybersecurity policy in the district.

### Rutland City School District: $26,836

Grant funds will enable the district to offer additional privacy and security training and awareness programs for end users. The staff training will better inform them of cybersecurity

threats such as malicious downloads, malware/ransomware, and phishing emails. Information gathered by this training will enable the district to update their current data security policy to include recommended procedures and systems. The work also will enable the district to focus their efforts and implement best practices in creating key elements of a security response plan.

### Two Rivers Supervisory Union: $29,340

The district will engage the services of an outside consultant to confirm and prioritize top network and data risks. The consultant will assist the district in developing the needed policies and procedures for detecting and responding to cybersecurity events.

### Washington Central Unified Union School District: $30,000

The district will use grant fund to expand on the knowledge gained from a previous cybersecurity incident. Funds will enable the district to implement a number of processes and practices to increase data security and network cybersecurity. Work under this grant will enable the district to create a data security and network cybersecurity policy and improve incident response planning. Funds will be used to conduct vulnerability and penetration testing, detection of anomalies, and DDOS mitigation to ensure network configurations and device update practices are effective.