**SAMPLE Cybersecurity Annex**

***Suggested content.***

***Customize the Annex to meet the needs of your district and/or school.***

***Include additional relevant information.***

*Consider cross-referencing the information included in your Data Security and Privacy Policy and your Parents' Bill of Rights for Data Privacy and Security as required by* [*NYS Ed Law §2-d*](https://www.nysenate.gov/legislation/laws/EDN/2-D) *and CR* [*Part 121*](https://www.nysed.gov/sites/default/files/programs/data-privacy-security/part-121.pdf)*.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Before** | | | |
| **Goal** | Create systems and policies to prevent cybersecurity incidents such as a data breach or ransomware attack. | | |
| **Objective(s)** | * Protect data from exposure and/or damage. * Educate district and school level stakeholders on cybersecurity threats. * Communicate procedures to prevent cybersecurity incidents. | | |
| **Courses of Action** | | | |
| **Who is Responsible** | **Action** | **Due Date** | **Follow Up Required** |
|  | Make the district/school aware of their assets and vulnerabilities. |  |  |
|  | Create and communicate actions to be taken in the event of a cybersecurity incident. |  |  |
|  | Conduct tabletop exercise with Emergency Response team and IT team. |  |  |
|  | Align cybersecurity incident procedures with requirements in district insurance policies; create awareness of the policies and implications of deviations from the policies. |  |  |
|  | Create processes for backing up data in the event of a systemwide attack. |  |  |
|  |  |  |  |
| **During** | | | |
| **Goal** | Analyze, contain, and eradicate the incident. | | |
| **Objective(s)** | Take immediate action to:   * Stop further damage. * Identify impacted technology/systems. * Identify impacted people. * Identify compromised data and the potential impact. * Identify what caused the incident. | | |
| **Courses of Action** | | | |
| **Who is Responsible** | **Action** | | |
|  | Enact protocols for responding to a cybersecurity incident. | | |
|  | Consult with school legal counsel and cyber insurance carrier. Develop message regarding the incident. | | |
|  | Communicate with internal stakeholders (i.e., staff, students, families, etc.). | | |
|  | Determine affected systems and develop a plan to mitigate (i.e., how to respond if systems are inoperable such as computers, phones, other) | | |
|  | Determine the Functional Annexes that may be activated during a cybersecurity breach include:   * Communication Plan * Continuity of Operations Plan * Early Dismissal Plan * Recovery Plan | | |
|  |  | | |
| **After** | | | |
| **Goal** | Restore systems. | | |
| **Objective(s)** | * Communicate with stakeholders. * Take action to prevent future incidents. | | |
| **Courses of Action** | | | |
| **Who is Responsible** | **Action** | | |
|  | Conduct post-incident analysis. | | |
|  | Communicate with all internal stakeholders (i.e., staff, students, families, etc.). | | |
|  | Communicate with all external stakeholders (i.e., legal counsel, IT contractors, insurance carriers, etc.). | | |
|  | Restore community confidence in the school’s ability to protect systems and data from another attack. | | |
|  | Provide accurate reporting to state and federal agencies within required time frames. | | |
|  | Conduct a “Lessons Learned” briefing. | | |
|  | Revise policies and procedures as deemed necessary. | | |
|  | Update Cybersecurity Annex. | | |
|  |  | | |