Incident Response Communications Plan

An incident response procedure is fundamental to any security program. In the event of a data security incident, communications – internal and external – are critically important and must be managed properly. Any incident response plan should include a process for communicating pertinent information about the incident to appropriate internal stakeholders, external stakeholders involved in any investigation, and to impacted individuals, parents and other community members in accordance with state laws and school system policies.

The incident response procedure should make clear who is responsible for communications, including ensuring that public notification is conducted in accordance with regulations and determining how that is to be accomplished. Communications templates, to be customized in the event of an incident, are also recommended.

This resource assumes that you have an incident response plan in place. However, if you don't, start by doing your homework. Leverage nationally recognized guidance to support development of your incident response plan. For example, NIST Computer Security Incident Handling Guide and the NIST Incident Response Recommendations and Considerations for Cybersecurity Risk Management provide foundational information and guidance to building an incident response plan and managing system and data security incidents. Identify your internal and external support teams, develop your plan, train (and train again), and adjust your plan based on the training outcomes.

This resource also supports: Trusted Learning Environment Security Practice 5:
The school system has a process in place to communicate data incidents to appropriate stakeholders, in accordance with state law and school system policies.

Examples of Evidence for the Trusted Learning Environment Application:
Incident response procedure that includes a communications plan, explaining who is responsible for ensuring that notification is conducted in accordance with applicable regulation and district policy, and how that is accomplished.

Additional resources are available from the US Department of Education's Privacy Technical Assistance Center, including:

- Data Breach Response Checklist
- Data Breach Scenario Trainings

When it comes to communications about an incident, here are 10 steps to consider:

1. **Make Your Contact List**. You can't run an incident without knowing how to contact your internal and external support teams without knowing how to reach them, 24/7, including holidays. Gather up phone numbers of your internal team and external supports. External supports could include:
    - Legal counsel or ideally, cybersecurity counsel (if you have either one of those);
    - Cybercrimes unit of local law enforcement (if one exists) and the local or regional cybercrimes division of the FBI;
    - Forensics firm that your district counsel has contracted with (or ideally, that your legal counsel has contracted with on behalf of your district) for the purpose of

incident response support, in case needed.

The contact list should be maintained as part of or adjacent to the incident response plan.

2. **Understand your legal obligations**. Your state likely has a breach notification law. It is very likely that the law only addresses notification requirements when there is unauthorized access that is likely to cause injury to an individual in the form of financial harm or identity theft, as might happen when there is access to unencrypted social security numbers, driver's license numbers, health information, or information that would permit access to an account. However, the laws vary and every state has its own requirements. Find your state breach notification law and get clear on the requirements. If you have legal counsel, they can provide this too.

3. **Consider the students.** Some states have breach notification laws that are specific to student data, but many do not. If your state has such legal requirements, add that to your work in item 2. If those requirements don't exist in your state, would your district provide notification to impacted individuals regardless? CoSN recommends that you do. It's the right thing to do. Besides, the local press will likely find out about it anyway, and it's important to maintaining community trust. Best to not be caught flat-footed. Work with your superintendent now to develop a policy on this front.

4. **Decide who will communicate**. In the event of an incident that requires communications to impacted individuals, the press, or both, to avoid confusion and miscommunication, and to help convey a sense of leadership and control, communications should come from one voice. Ideally, the voice is that of your superintendent. This should be articulated in your incident response plan.

5. **Consider employee behavior**. Your incident response plan and security training should include how you expect employees to report suspicious activity. However, what do you want them to do after they report it? Remind your employees that suspicious activity is serious, and not fodder for hallway chatter. Consider how you might want the reporter to behave after the report, and if you might want to keep that individual updated so that they know what to expect if the time comes.

6. **Write the notifications now.** The best time to draft communications informing parents, students, or employees of a breach impacting their personal information while conveying a sense of calm (as much as that is possible with this type of news) and control over the situation is not during an incident when the adrenaline may be pumping. Draft these now, before there's an incident. Consider what you would say and how you would say it. Include placeholders for facts specific to the incident as you know them. This might include placeholders for when the incident was discovered, what data elements were involved and over how many years, how many individuals have been impacted, whether the incident has been contained, what is being done to prevent such an incident in the future, what supports are available to impacted individuals, if appropriate, and any other information required by law.

   You will redraft these – or parts of these – in the event of an incident, but sample messages that you keep in your incident response plan will help you capture the right tone

and remind you of the facts that may need to be disclosed in the event of an incident.

7. **Write press holding statements now.** Security incidents are big news, particularly to local reporters. (In some cases, you may even learn about a security incident from a reporter.) Draft "holding" statements for the designated incident response communicator to use in responding to press inquiries before all facts are known. These are typically brief statements that can be issued in a crisis as an alternative to "no comment." They're often used when reporters are asking questions before you have all the facts on hand to make a formal and more thorough disclosure.

   When done properly, these can go a long way to helping keep the community calm. Typically, these statements involve acknowledging that there is an incident (if that is the case), expressing an appropriate tone of sympathy for those who may be impacted, and noting that action is being taken to address the situation and that further communications will be forthcoming. You will, of course, customize such statements in the event of a breach, but as with notification to impacted individuals, the best time to draft some placeholder language to address a crisis is when you're not actually in a crisis.

8. **Consider how the messages might be received.** Once you've drafted your placeholder notification letters and press holding statements, review them again, considering only how the recipient might receive the news. Is there anything in your drafts that overplays or underplays the incident? Is it appropriately reassuring without sugar-coating the situation? Is the information communicated effectively? Remember your objectives are to meet legal requirements, meet policy requirements your district may have put in place for incident response communications that go beyond what the law requires, and convey the facts. Communications that have the potential to stir up emotions unnecessarily, which doesn't help anyone. Pay attention to the facts and the tone.

9. **Strike the right balance.** The timing of incident response communications can be tricky. You want to notify impacted individuals as soon as possible, while at the same time, you need to ensure your communications don't compromise an ongoing investigation. For example, you need to move deliberately and thoughtfully through what may likely be the complex work of containing an incident before communicating about it. This includes taking the time needed to gather and document evidence, including taking screenshots and creating appropriately detailed logs of the response milestones.

   When training on your incident response plan, set up a training session specifically focused on communications. Since your superintendent should be the one authorized to communicate, it will be important that they have the information they need to decide on timing of that communication, including timing required under applicable laws. Consider how you will coordinate between technical work being done to contain an incident and timing of communications.

10. **Stay calm.** Bear in mind that in the event of a security incident or breach that is made public or that otherwise requires notification is your district's responsibility. You may call in local law enforcement, the FBI, CISA, or others to support your district, but to your community, YOU are the authority on their students' data. For them, the cavalry isn't coming. You ARE the calvary. Remember to keep your team calm and focused while

responding to an incident. It'll help you ensure that you're getting the right facts to the right people to decide when and how to communicate responsibly to the public.