Minimum Standards for Privacy and Security of Student and Employee Data
New Hampshire Department of Education

# FREQUENTLY ASKED QUESTIONS

## 1. What is meant by "Minimum Standards"?

The "Minimum Standards for Privacy and Security of Student and Employee Data" (hereafter referred to simply as the "Minimum Standards") are security and privacy requirements which must be implemented on your information systems and networks which process, store or transmit any of the types of data identified in section 1.B.

a. Are any of these standards optional?

No, none of the Minimum Standards are optional. The Minimum Standards as a whole establish the minimally acceptable baseline of security and privacy.

## 2. Could you explain the "Applicability" of the Minimum Standards?

Section 1 of the document defines the WHO and WHAT that the Minimum Standards apply to, as well as their purpose. The Minimum Standards apply to all local education agencies who fall under the purview of RSA 189:66 and the New Hampshire Department of Education. From a technical perspective, the Minimum Standards apply specifically to those information systems, servers, workstations, storage devices (including portable and mobile), printers, and networking devices which process, store or transmit the types of information identified in section 1.B.

As an example, consider a school network which has workstations, servers, printers and network devices which collectively either process, store or transmit student or teacher personally identifiable data, or perhaps these devices do all three (process, store and transmit). The Minimum Standards must be applied to all of this information technology (IT) equipment – none of the devices are exempt from the Minimum Standards. In a network environment, you should assume that **all devices** which support the processing of the student or teacher data must implement the Minimum Standards.

Consider on the other hand the case of an "isolated" or "standalone" system. This would be defined as one or more machines that **are not connected** to the school network, and more importantly, **do not process, store or transmit** any of the student, teacher or "covered" data. In this example, the Minimum Standards would not have to be applied. An example of this could be a single PC that serves an administrative or logistical function for the school, but does not handle any student, teacher or covered data, and furthermore, is not connected to the school network that does handle student data. So long as the machine does not handle the sensitive data and is not connected to other machines which do handle the data, the Minimum Standards would not apply to that single machine.

Here is another example of an isolated system. Let's say the school has an Internet connection from an ISP **which does not connect to the main school network**, but instead connects to a dozen or so workstations in a technology lab. Assume the lab

## FREQUENTLY ASKED QUESTIONS

machines have software tools for learning computer programming, and these machines connect to an Internet site with computer science educational material. So long as the computer programming applications and the Internet sites that the students connect to as part of the lab do not collect, process, store or transmit student, teacher or other "Covered information" as described in section 1.B, these lab machines **would not have to** implement the Minimum Standards. But as soon as students in the learning lab environment have to create accounts which identify them by name and in the process of the educational program, collects or records other student data, the Minimum Standards would apply. Furthermore, if the computer lab is connected to the school network, it will be hard to argue that no student, teacher or "Covered Information" is ever collected, processed or stored on the lab machines, so in that event, the lab machines would also have to comply with the Minimum Standards.

3. **Do the Minimum Standards apply to vendor hosted applications or service providers?**

   Yes, if the vendor hosted applications or service providers collect, process, store or transmit any of the student, teacher or other "Covered Information" identified in section 1.B. This requirement is also highlighted in RSA 189:66, V.e.

4. **How are the Minimum Standards related to FERPA?**

   They are complementary in nature.

   The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records.

   The Minimum Standards are much more specific and technical in nature, and apply more specifically in the configuration of IT systems and networks which handle student data, while FERPA provides a higher level focus on privacy rights and protections covering dissemination and disclosure.

5. **The underlying NIST publication SP 800-171 says that it is for protecting "Controlled Unclassified Information" or CUI – how does that relate to student records and the Minimum Standards?**

   "Controlled Unclassified Information" or CUI was defined in 32 CFR (Code of Federal Regulations) part 2002, to establish policy for agencies on designating, safeguarding,

## FREQUENTLY ASKED QUESTIONS

disseminating, marking, decontrolling, and disposing of CUI. Furthermore, the CUI Registry established the category of "Student Records" relative to education records that are directly related to a student under FERPA as a type of information to be protected as Controlled Unclassified Information. Therefore, NIST SP 800-171, "*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*" has a direct relationship to the CUI category of "student records" and thus serves as the best underlying federal guidance to apply to the Minimum Standards.

It should be emphasized that **not all security requirements** from NIST SP 800-171 were incorporated into the Minimum Standards – but rather that the Minimum Standards represent a core subset of the security requirements from NIST SP 800-171. Some of the more rigorous or stringent security requirements from NIST SP 800-171 were omitted from the Minimum Standards due to the level of difficulty they would have imposed on all schools, therefore the end result represents a **tailored set** of security requirements for schools to implement.

**6. How will the Minimum Standards be enforced, and by whom?**

As described in RSA 189:66, paragraph V, each local education agency is to develop a data and privacy governance plan which is to be presented to the school board for review and approval by June 30, 2019, and will be updated annually. The data and privacy governance plan should include the school's progress and status in implementing the Minimum Standards, along with other requirements as described in items RSA 189:66, V.a through V.e.

**7. Will the State audit compliance with the Minimum Standards?**

At the present time, the state has not established a program to audit compliance with the Minimum Standards.

**8. Can our school/school district implement more rigorous security or privacy protections?**

Yes, a school or school district may implement more rigorous (stringent) security or privacy protections at their discretion. The school should consult with their school board and reflect this approach in their data and privacy governance plan.

**9. How soon will we have to implement all of the Minimum Standards?**

# FREQUENTLY ASKED QUESTIONS

Although the Revised Statute requires that local education agencies "shall develop a data and privacy governance plan which shall be presented to the school board for review and approval by June 30, 2019," RSA 189:66 does not mandate full compliance by a specific date. It is expected that each local education agency will continue to make progress in their implementation of the Minimum Standards, and will reflect this status in their annual reporting to the school board, to include the results from periodic risk assessments.

**10. How can we measure/assess our implementation of the Minimum Standards?**

Since each of the Minimum Standards map back to a specific security or privacy requirement in NIST SP 800-171, schools can download NIST SP 800-171 and NIST SP 800-171A from the NIST website. NIST SP 800-171A, titled "*Assessing Security Requirements for Controlled Unclassified Information*" provides process and procedures to assess each security requirement or sub-requirement as described in NIST SP 800-171. Additionally, if the school engages a cyber-security vendor to conduct either a security assessment, risk assessment or both, the vendor should be asked to assess compliance against the Minimum Standards and the companion security requirements from NIST SP 800-171.

**11. Can I map these standards back to NIST SP 800-53 security controls?**

Yes. NIST SP 800-171, Appendix D has a table which maps the 800-171 security requirements (which the Minimum Standards are based upon) to the corresponding NIST SP 800-53 Security Controls.

**12. Do I need to retain an attorney to assist in the implementation of the Minimum Standards or a risk assessment?**

No, retaining an attorney is not required to assist in the implement of the Minimum Standards or a risk assessment.

**13. What if I still have questions about interpreting or implementing the Minimum Standards?**

Please contact the New Hampshire Department of Education.