VIOLACIÓN DE LA SEGURIDAD Y NOTIFICACIÓN

La Junta de Educación está comprometida a proteger la información privada que posea de los estudiantes, el personal y los residentes del Distrito Escolar de la Ciudad de Rochester. Los sistemas de información del Distrito están protegidos por un firewall avanzado de próxima generación, seguridad de punto final y escaneo de correo electrónico. Sin embargo, la naturaleza cambiante de la tecnología y el beneficio potencial de comprometer los sistemas de información impiden que cualquier sistema sea absolutamente inviolable. En caso de que los registros del Distrito se vean comprometidos o se adquiera información privada sin autorización, el Distrito deberá cumplir con la Ley de Notificación y Violación de la Seguridad de la Información y esta política.

La Junta de Educación reconoce la creciente preocupación por el aumento de los robos de identidad y la necesidad de redes seguras y de una notificación rápida cuando se produzcan violaciones de la seguridad. La Junta adopta el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología Versión 1.1 (NIST CSF) para la seguridad y protección de datos. Los sistemas del Distrito seguirán como mínimo el NIST CSF y adoptarán tecnologías, salvaguardas y prácticas que se alineen con esta versión del Instituto Nacional de Estándares. Esto incluirá una evaluación del estado actual de la ciberseguridad del Distrito, su futuro estado de ciberseguridad objetivo, las oportunidades de mejora, el progreso hacia el estado objetivo y la comunicación sobre el riesgo de ciberseguridad.

El Distrito designará un Oficial de Protección de Datos para que sea responsable de la implementación de las políticas y procedimientos requeridos en la Ley de Educación §2-d y sus regulaciones adjuntas, y para que sirva como punto de contacto para la seguridad de los datos.

Definiciones

Información personal: cualquier información relativa a una persona física que, por su nombre, número, símbolo, marca u otro identificador, pueda usarse para identificar a dicha persona física.

Información privada: información personal, que no está codificada, que incluye uno o más de los siguientes datos:

1. número de la seguridad social

2. número de licencia de conducir o tarjeta de identificación de no conductor de vehículos;

3. domicilio, número de teléfono, dirección de correo electrónico personal, números de identificación de usuario o contraseñas de cuentas electrónicas personales; o

4. número de cuenta, número de tarjeta de crédito o débito, en combinación con cualquier código de seguridad, código de acceso o contraseña requeridos que permitan el acceso a la información personal de un empleado o estudiante, registros de empleo, registros académicos o cuenta financiera.

Bajo el Título I de la Ley de Educación Primaria y Secundaria, el Distrito está obligado a dar información del directorio de estudiantes a los reclutadores de las universidades, los posibles empleadores, y los servicios militares. Los padres deben notificar al Distrito si no desean que la información del directorio de su hijo sea compartida con los reclutadores. (Vea la política de Reclutamiento por Organizaciones con Membresía Restrictiva o Prácticas de Empleo Autorizadas y Permitidas por la Ley (1240.1) para más información). La información del directorio de estudiantes incluye: dirección del estudiante, número de

teléfono, fecha y lugar de nacimiento, nombre de la última escuela a la que asistió, fechas de asistencia, área de estudio y participación en actividades atléticas y extracurriculares.

La "información privada" no incluye la información públicamente disponible que se pone legalmente a disposición del público en general de los registros del gobierno federal, estatal o local.

La Junta ordena al Superintendente de Escuelas, de acuerdo con el personal apropiado de administración y tecnología establecer reglamentos que traten lo siguiente:

1. la protección de la "información personal identificable" de estudiantes y maestro/directores de escuelas conforme a la Ley de Educación §2-d y la Parte 121 del Comisionado de Educación;

2. la protección de la "información privada" en virtud de la Ley Estatal de Tecnología §208 y la Ley SHIELD de Nueva York; y

3. los procedimientos para notificar a las personas afectadas por violaciones o accesos no autorizados a información protegida.

Violación de la Seguridad del Sistema: adquisición no autorizada de datos informáticos que comprometa la seguridad, confidencialidad o integridad de la información personal. La adquisición de buena fe de información personal por parte de un empleado o agente de una entidad estatal para los fines de la agencia no constituye una violación de la seguridad del sistema, siempre que la información privada no se use ni esté sujeta a divulgación no autorizada.

El Superintendente establecerá reglas relativas a los procedimientos que se utilizarán para:

1. identificar cualquier violación de seguridad que resulte en la divulgación de información privada;

2. garantizar la formación continua de los empleados del Distrito en materia de seguridad de las tecnologías de la información; e

3. informar al Jefe de Comunicaciones, que es responsable de notificar a todas las personas afectadas por la violación de la seguridad.

Notificación de incumplimiento

Una vez sea descubierta una violación del sistema de seguridad informático, el Director de Comunicaciones del Distrito o su designado notificará a las personas afectadas sobre dicha violación. Las personas afectadas incluirán todas las personas cuya información privada fue, o se cree razonablemente que fue, adquirida sin una autorización válida. La divulgación se realizará en el tiempo más rápido posible, de acuerdo con las necesidades legítimas de las autoridades o cualquier medida necesaria para determinar el alcance de la violación y restaurar la integridad razonable del sistema de datos.

El Director de Comunicaciones del Distrito dará todas las notificaciones requeridas por esta política e incluirá información de contacto en el Distrito para responder a las preguntas sobre la violación y una descripción de las categorías de información que fueron, o se cree razonablemente que fueron, adquiridas sin autorización. El Jefe de Comunicaciones dará dicha notificación directamente a las personas afectadas mediante uno de los siguientes métodos:

1. notificación por escrito;

2. aviso electrónico; o

3. notificación telefónica.

La notificación debe brindarse de una manera que razonablemente se espera que sea recibida por las personas afectadas. El Distrito debe mantener un registro de todas las personas notificadas bajo esta política.

El Director de Comunicaciones también notificará cualquier incumplimiento, su momento y el número aproximado de personas afectadas al Fiscal General del Estado de Nueva York, a la Junta de Protección al Consumidor del Estado de Nueva York y a la Oficina de Seguridad Cibernética y Asuntos Críticos del Estado de Nueva York. Infraestructura.

En el caso de que se notifique a más de cinco mil residentes de Nueva York al mismo tiempo, el Distrito también notificará a las agencias de informes del consumidor sobre el momento, el contenido y la distribución de los avisos y el número aproximado de personas afectadas.

Contratistas externos: El Distrito se asegurará de que los contratos con contratistas externos reflejen que la confidencialidad de la PII de cualquier estudiante y/o maestro o director de escuela se mantendrá de acuerdo con las leyes federales y estatales y la política de privacidad y seguridad de datos del Distrito.

Cada contratista externo que vaya a recibir datos de estudiantes o de maestros o directores deberá:

1. adoptar tecnologías, salvaguardas y prácticas que se alineen con el NIST CSF;

2. cumplir la política de seguridad y privacidad de datos del Distrito y las leyes aplicables que afecten al Distrito;

3. limitar el acceso interno a la PII únicamente a aquellos empleados o subcontratistas que necesiten acceder para prestar los servicios contratados;

4. no utilizar la PII para ningún fin que no esté explícitamente autorizado en su contrato

5. no revelar ninguna PII a terceros sin el consentimiento previo por escrito de los padres o del estudiante elegible (es decir, estudiantes de dieciocho años o mayores):

   a. excepto para los representantes autorizados del contratista externo en la medida en que estén ejecutando el contrato; o
   b. a menos que lo exija la ley o una orden judicial y el contratista externo proporcione un aviso de divulgación al Distrito, a menos que se prohíba expresamente.

6. mantener salvaguardas administrativas, técnicas y físicas razonables para proteger la seguridad, confidencialidad e integridad de la PII bajo su custodia;

7. utilizar la encriptación para proteger la PII bajo su custodia; y

8. no vender, utilizar o divulgar la PII con fines comerciales o de marketing, ni facilitar su uso o divulgación a terceros con fines comerciales o de marketing, ni permitir que terceros lo hagan. Los contratistas externos pueden divulgar la PII a subcontratistas contratados para cumplir las obligaciones del contratista, pero dichos subcontratistas deben respetar las obligaciones de protección de datos.

Si el contratista externo comete un incumplimiento o una divulgación no autorizada de PII, notificará de inmediato al Distrito de la manera más pronta posible, sin demoras irrazonables, pero no más de siete días calendario después del descubrimiento del incumplimiento.

Plan de privacidad y seguridad de datos de contratistas externos: El Distrito se asegurará de que los contratos con todos los contratistas externos incluyan el plan de privacidad y seguridad de datos del contratista externo. Este plan debe ser aceptado por el Distrito.

Como mínimo, cada plan deberá:

1. describir cómo se cumplirán todos los requisitos contractuales de seguridad y privacidad de datos estatales, federales y locales durante la vigencia del contrato, en consonancia con esta política;

2. especificar las salvaguardias y prácticas que ha implantado para proteger la PII

3. demostrar que cumple los requisitos de la Sección 121.3(c) de esta Parte;

4. especificar cómo reciben o recibirán formación sobre las leyes federales y estatales que rigen la confidencialidad de dichos datos las personas que tienen acceso a los datos de estudiantes y/o maestros o directores antes de recibir dicho acceso;

5. especificar si el contratista externo utilizará subcontratistas y cómo gestionará esas relaciones y contratos para garantizar la protección de la información de identificación personal;

6. especificar cómo gestionará el contratista externo los incidentes relacionados con la seguridad y la privacidad de los datos que afecten a la información de identificación personal, incluida la especificación de cualquier plan para identificar infracciones y divulgaciones no autorizadas, y para notificarlas de inmediato al Distrito;

7. describir si, cómo y cuándo los datos serán devueltos al Distrito, transferidos a un contratista sucesor, a petición del Distrito, borrados o destruidos por el contratista tercero cuando el contrato haya terminado o expire.

Ref. cruzada: Registros del Distrito Escolar (1120)
Relaciones con los medios de comunicación (1130)
Reclutamiento por organizaciones con membresía o prácticas laborales restrictivas autorizadas y permitidas por la ley (1240.1)
Políticas de Internet (4526)

Ref: Ley Estatal de Tecnología §§201-208
Derecho Laboral §203-d

Notas: Adoptada el 22 de junio de 2011 mediante Resolución No. 2010-11: 906; Modificado el 26 de julio de 2018 mediante la Resolución No. 2018-19: 80; Modificado el 20 de octubre de 2022 de conformidad con la Resolución No. 2022-23: 206

ct/rp