सुरक्षा उल्लङ्घन र अधिसूचना

शिक्षा बोर्ड रोचेस्टर सिटी स्कूल डिस्ट्रिक्टका विद्यार्थीहरू, कर्मचारीहरू र जिल्लाको स्वामित्वमा रहेका बासिन्दाहरूको निजी जानकारीको सुरक्षा गर्न प्रतिबद्ध छ। जिल्लाको सूचना प्रणालीहरू उन्नत नेक्स्ट जेनरेशन फायरवाल सुरक्षा, अन्तिम बिन्दु सुरक्षा, र इमेल स्क्यानिङद्वारा सुरक्षित छन्। यद्यपि, प्रविधिको विकसित प्रकृति र सम्झौता सूचना प्रणालीबाट हुने सम्भावित लाभले कुनै पनि प्रणालीलाई पूर्णतया अपरिहार्य हुनबाट रोक्छ। यदि जिल्लाको अभिलेखमा सम्झौता गरिएको छ वा प्राधिकरण बिना निजी जानकारी प्राप्त गरिएको छ भने, जिल्लाले सूचना सुरक्षा उल्लङ्घन र सूचना ऐन र यो नीतिको पालना गर्नेछ।

शिक्षा बोर्डले पहिचान चोरीमा वृद्धि र सुरक्षा उल्लंघन हुँदा सुरक्षित नेटवर्क र तुरुन्त सूचनाको आवश्यकताको बारेमा बढेको चिन्तालाई स्वीकार गर्दछ। बोर्डले डाटा सुरक्षा र सुरक्षाको लागि मानक र टेक्नोलोजी साइबर सुरक्षा फ्रेमवर्क संस्करण १.१ (एनआइएसटि सिएसएफ) को लागि राष्ट्रिय संस्थान अपनाउछ। जिल्लाका प्रणालीहरूले न्यूनतम रूपमा एनआइएसटि सिएसएफ लाई पछ्याउनेछन र यससँग मिल्ने प्रविधि, सुरक्षा र अभ्यासहरू अपनाउनेछन्। यसमा जिल्लाको वर्तमान साइबर सुरक्षा अवस्था, तिनीहरूको लक्षित भविष्यको साइबर सुरक्षा अवस्था, सुधारका अवसरहरू, लक्षित राज्यतर्फको प्रगति, र साइबर सुरक्षा जोखिमको बारेमा सञ्चार समावेश हुनेछ।

जिल्लाले शिक्षा कानून §२-डि र यससँग सम्बन्धित नियमहरूमा आवश्यक नीति र प्रक्रियाहरूको कार्यान्वयनको लागि जिम्मेवार हुन र डाटा सुरक्षाको लागि सम्पर्क बिन्दुको रूपमा सेवा गर्नको लागि डेटा सुरक्षा अधिकारीलाई नियुक्त गर्नेछ।

परिभाषाहरू

व्यक्तिगत जानकारी: प्राकृतिक व्यक्तिको बारेमा कुनै पनि जानकारी जुन नाम, संख्या, चिन्ह, चिन्ह वा अन्य पहिचानकर्ताको कारणले त्यो प्राकृतिक व्यक्तिलाई पहिचान गर्न प्रयोग गर्न सकिन्छ।

निजी जानकारी: व्यक्तिगत जानकारी, जुन गुप्तिकरण गरिएको छैन, जसमा निम्न मध्ये एक वा बढी समावेश छन्:

१. सामाजिक सुरक्षा नम्बर;

२. चालकको इजाजतपत्र नम्बर वा गैर-चालक पहिचान कार्ड नम्बर;

३. घरको ठेगाना, टेलिफोन नम्बर, व्यक्तिगत इलेक्ट्रोनिक इमेल ठेगाना, प्रयोगकर्ता पहिचान नम्बर वा व्यक्तिगत इलेक्ट्रोनिक खाताहरूमा पासवर्डहरू; वा

४. खाता नम्बर, क्रेडिट वा डेबिट कार्ड नम्बर, कुनै पनि आवश्यक सुरक्षा कोड, पहुँच कोड, वा पासवर्डको संयोजनमा जसले कर्मचारी वा विद्यार्थीको व्यक्तिगत जानकारी, रोजगारी रेकर्ड, शैक्षिक रेकर्ड, वा वित्तीय खातामा पहुँच अनुमति दिन्छ।

प्राथमिक र माध्यमिक शिक्षा ऐनको शीर्षक I अन्तर्गत, जिल्लाले कलेजहरू, सम्भावित रोजगारदाताहरू, र सैन्य सेवाहरूबाट भर्ती गर्नेहरूलाई विद्यार्थी निर्देशिका जानकारी उपलब्ध गराउन आवश्यक छ। आमाबाबुले आफ्नो बच्चाको डाइरेक्टरी जानकारी भर्तीकर्ताहरूसँग साझा गर्न चाहँदैनन् भने जिल्लालाई सूचित गर्नुपर्छ। (थप जानकारीको लागि कानुन नीति (१२४०.१) द्वारा अधिकृत र अनुमति प्राप्त प्रतिबन्धात्मक सदस्यता वा रोजगार अभ्यासहरू भएका संगठनहरूद्वारा भर्ती हेर्नुहोस्)। विद्यार्थी डाइरेक्टरी जानकारीमा समावेश छ: विद्यार्थीको ठेगाना, टेलिफोन नम्बर, जन्म मिति र स्थान, पछिल्लो विद्यालयको नाम, उपस्थितिको मिति, अध्ययनको क्षेत्र, र एथलेटिक र अतिरिक्त क्रियाकलापहरूमा सहभागिता।

"निजी जानकारी" ले सार्वजनिक रूपमा उपलब्ध जानकारी समावेश गर्दैन जुन कानुनी रूपमा संघीय, राज्य, वा स्थानीय सरकारको रेकर्डबाट आम जनतालाई उपलब्ध गराइन्छ।

बोर्डले स्कूल सुपरिटेन्डेन्टलाई उपयुक्त व्यवसाय र प्रविधि कर्मीहरूको अनुसार नियमहरू स्थापना गर्न निर्देशन दिन्छ जुन सम्बोधन गर्दछ:

१. शिक्षा आयुक्तको शिक्षा कानून §२-डि र भाग १२१ अन्तर्गत विद्यार्थी र शिक्षक। प्रिन्सिपलको "व्यक्तिगत रूपमा पहिचान योग्य जानकारी" को सुरक्षा;

२. राज्य प्रविधि कानून §२०८ र **न्यूयोर्क शिल्ड ऐन** अन्तर्गत "निजी जानकारी" को सुरक्षा; र

३. उल्लंघन वा संरक्षित जानकारीको अनधिकृत पहुँचबाट प्रभावित व्यक्तिहरूलाई सूचित गर्ने प्रक्रियाहरू।

प्रणालीको सुरक्षाको उल्लङ्घन: कम्प्यूटरीकृत डाटाको अनधिकृत अधिग्रहण जसले व्यक्तिगत जानकारीको सुरक्षा, गोपनीयता, वा अखण्डतामा सम्झौता गर्दछ। एजेन्सीको उद्देश्यका लागि राज्य निकायको कर्मचारी वा एजेन्टले व्यक्तिगत जानकारीको राम्रो विश्वास प्राप्त गर्नु प्रणालीको सुरक्षाको उल्लङ्घन होइन, यदि निजी जानकारी प्रयोग गरिएको छैन वा अनधिकृत खुलासाको अधीनमा छ।
सुपरिटेन्डेन्टले प्रयोग गरिने प्रक्रियाहरूको सम्बन्धमा नियमहरू स्थापना गर्नेछ:

१. सुरक्षाको कुनै पनि उल्लङ्घनहरू पहिचान गर्नुहोस जुन निजी जानकारीको रिलीजको परिणाम हो;

२. सूचना प्रविधि सुरक्षा जागरूकता सम्बन्धी निरन्तर आधारमा जिल्ला कर्मचारीहरूलाई प्रशिक्षण प्रदान गरिएको सुनिश्चित गर्नुहोस्; र

३. संचार अधिकारीको प्रमुखलाई सूचित गर्नुहोस्, जो सुरक्षा उल्लङ्घनबाट प्रभावित सबै व्यक्तिहरूलाई सूचित गर्न जिम्मेवार छन्।

उल्लंघनको सूचना
जिल्लाको सञ्चार अधिकारी वा नियुक्त व्यक्तिले आफ्नो कम्प्युटर प्रणाली(हरू) को सुरक्षाको कुनै पनि उल्लङ्घनको खोजी पछि प्रभावित व्यक्तिहरूलाई सूचित गर्नेछ। प्रभावित व्यक्तिहरूमा सबै व्यक्तिहरू समावेश हुनेछन् जसको निजी जानकारी वैध प्राधिकरण बिना प्राप्त गरिएको थियो, वा उचित रूपमा विश्वास गरिएको थियो। खुलासा सम्भव भएसम्म उपयुक्त समयमा, कानून प्रवर्तनको वैध आवश्यकताहरू वा उल्लङ्घनको दायरा निर्धारण गर्न र डाटा प्रणालीको उचित अखण्डता पुनर्स्थापना गर्न आवश्यक कुनै पनि उपायहरूसँग सुसंगत गरिनेछ।

जिल्लाको सञ्चार अधिकारीले यस नीतिद्वारा आवश्यक सबै सूचनाहरू उपलब्ध गराउनेछ र उल्लङ्घन सम्बन्धी प्रश्नहरूको जवाफ दिनको लागि जिल्लामा सम्पर्क जानकारी समावेश गर्नेछ र जानकारीको कोटीहरूको विवरण जुन थियो, वा भएको मानिन्छ, प्राधिकरण बिना अधिग्रहण। सञ्चार अधिकारीले यस्तो सूचना प्रत्यक्ष रूपमा प्रभावित व्यक्तिहरूलाई निम्न मध्ये कुनै एक विधिद्वारा उपलब्ध गराउनु पर्नेछ:

१. लिखित सूचना;

२. इलेक्ट्रोनिक सूचना; वा

३. टेलिफोन सूचना।

सूचना प्रभावित व्यक्तिहरूबाट प्राप्त हुने अपेक्षा गरिएको रूपमा उपलब्ध गराउनुपर्छ। जिल्लाले यस नीति अन्तर्गत सूचित सबै व्यक्तिहरूको लग राख्नुपर्छ।

सञ्चार अधिकारीका प्रमुखले कुनै पनि उल्लङ्घन, यसको समय, र प्रभावित व्यक्तिहरूको अनुमानित संख्या न्यूयोर्क राज्य महान्यायाधिवक्ता, न्यूयोर्क राज्य उपभोक्ता संरक्षण बोर्ड, र साइबर सुरक्षा र गम्भीर न्यूयोर्क राज्य कार्यालयलाई पनि सूचना पूर्वाधार प्रदान गर्नेछ।

एकै पटकमा पाँच हजारभन्दा बढी न्यूयोर्कका बासिन्दाहरूलाई सूचित गर्नु पर्ने अवस्थामा, जिल्लाले उपभोक्ता रिपोर्टिङ एजेन्सीहरूलाई सूचनाहरूको समय, सामग्री र वितरण र प्रभावित व्यक्तिहरूको अनुमानित संख्याको रूपमा पनि सूचित गर्नेछ।

तेस्रो-पक्ष ठेकेदारहरू: जिल्लाले यो सुनिश्चित गर्नेछ कि तेस्रो-पक्ष ठेकेदारहरूसँगको सम्झौताले संघीय र राज्य कानून र जिल्लाको डेटा सुरक्षा र गोपनीयता नीति अनुसार कुनै पनि विद्यार्थी र।वा शिक्षक वा प्रिन्सिपल पिII को गोपनीयतालाई प्रतिबिम्बित गर्दछ।

प्रत्येक तेस्रो-पक्ष ठेकेदार जसले विद्यार्थी डेटा वा शिक्षक वा प्रिन्सिपल डेटा प्राप्त गर्नेछ:

१. एनआइएसटि सिएसएफ सँग मिल्ने प्रविधि, सुरक्षा र अभ्यासहरू अपनाउने;

२. जिल्लाको डाटा सुरक्षा र गोपनीयता नीति र जिल्लालाई प्रभाव पार्ने लागू कानूनहरूको पालना गर्नुहोस्;

३. पिII को आन्तरिक पहुँच केवल ती कर्मचारी वा उप-ठेकेदारहरूलाई सीमित गर्नुहोस जसलाई अनुबंधित सेवाहरू प्रदान गर्न पहुँच चाहिन्छ;

४. कुनै पनि उद्देश्यको लागि पिII प्रयोग नगर्नुहोस यसको सम्झौतामा स्पष्ट रूपमा अधिकृत छैन;

५. अभिभावक वा योग्य विद्यार्थीको पूर्व लिखित सहमति बिना कुनै पनि अन्य पक्षलाई कुनै पनि पिII खुलासा नगर्नुहोस (अर्थात, अठार वर्ष वा माथिका विद्यार्थीहरू):

क. तेस्रो-पक्ष ठेकेदारका अधिकृत प्रतिनिधिहरू बाहेक उनीहरूले सम्झौता पूरा गरिरहेको हदसम्म; वा

ख. जबसम्म कानून वा अदालतको आदेश द्वारा आवश्यक पर्दछ र तेस्रो-पक्ष ठेकेदारले जिल्लालाई खुलासाको सूचना प्रदान गर्दछ, स्पष्ट रूपमा निषेध नगरेसम्म।

६. यसको हिरासतमा रहेको पिII को सुरक्षा, गोपनीयता र अखण्डताको रक्षा गर्न उचित प्रशासनिक, प्राविधिक र भौतिक सुरक्षाहरू कायम राख्नुहोस्;

७. पिII लाई आफ्नो हिरासतमा सुरक्षित गर्न इन्क्रिप्सन प्रयोग गर्नुहोस्; र

८. कुनै पनि मार्केटिङ वा व्यावसायिक उद्देश्यका लागि पिII बेच्ने, प्रयोग गर्ने वा खुलासा नगर्ने, मार्केटिङ वा व्यावसायिक उद्देश्यका लागि अरूले यसको प्रयोग वा खुलासा गर्न सहज बनाउने, वा अर्को पक्षलाई त्यसो गर्न अनुमति दिने। तेस्रो पक्ष ठेकेदारहरूले ठेकेदारको दायित्वहरू पूरा गर्न संलग्न उप-ठेकेदारहरूलाई पिII जारी गर्न सक्छन्, तर त्यस्ता उप-ठेकेदारहरूले राज्य र संघीय कानूनको डेटा सुरक्षा दायित्वहरू, र जिल्लासँगको सम्झौताको पालना गर्नुपर्छ।

यदि तेस्रो-पक्ष ठेकेदारले पिII को उल्लङ्घन वा अनाधिकृत रूपमा जारी गरेको छ भने, यसले तुरुन्तै डिस्ट्रिक्टलाई अव्यावहारिक ढिलाइ नगरी सम्भव भएसम्म सबैभन्दा उपयुक्त तरिकामा सूचित गर्नेछ तर उल्लङ्घन पत्ता लगाएको सात क्यालेन्डर दिनहरू भन्दा बढी छैन।

तेस्रो-पक्ष ठेकेदारहरूको डेटा सुरक्षा र गोपनीयता योजना: जिल्लाले सबै तेस्रो-पक्ष ठेकेदारहरूसँगको सम्झौतामा तेस्रो-पक्ष ठेकेदारको डेटा सुरक्षा र गोपनीयता योजना समावेश छ भनी सुनिश्चित गर्नेछ। यो योजना जिल्लाले स्वीकार गर्नुपर्छ।

न्यूनतममा, प्रत्येक योजना निम्न हुनेछ:

१. यस नीतिसँग सुसंगत, सबै राज्य, संघीय, र स्थानीय डेटा सुरक्षा र सम्झौताको जीवनमा गोपनीयता अनुबंध आवश्यकताहरू कसरी पूरा गरिनेछ भनेर रूपरेखा;

२. पिII लाई सुरक्षित गर्नको लागि यसमा भएका सुरक्षा र अभ्यासहरू निर्दिष्ट गर्नुहोस्;

३. यसले यस भागको खण्ड १२१.३(सि) को आवश्यकताहरू पूरा गर्दछ भनेर देखाउनुहोस्;

४. विद्यार्थी र ।वा शिक्षक वा प्रिन्सिपल डेटामा पहुँच भएका व्यक्तिहरूले पहुँच प्राप्त गर्नु अघि त्यस्ता डेटाको गोपनीयतालाई नियन्त्रण गर्ने संघीय र राज्य कानूनहरूमा कसरी प्रशिक्षण प्राप्त गर्छन वा प्राप्त गर्छन भनेर निर्दिष्ट गर्नुहोस्;

५. यदि तेस्रो-पक्ष ठेकेदारले उप-ठेकेदारहरू प्रयोग गर्नेछ र व्यक्तिगत रूपमा पहिचान योग्य जानकारी सुरक्षित छ भनेर सुनिश्चित गर्न ती सम्बन्धहरू र सम्झौताहरू कसरी व्यवस्थापन गर्नेछ भनेर निर्दिष्ट गर्नुहोस्;

६. उल्लङ्घन र अनाधिकृत खुलासाहरू पहिचान गर्ने योजनाहरू निर्दिष्ट गर्ने, र जिल्लालाई तुरुन्तै सूचित गर्ने सहित व्यक्तिगत रूपमा पहिचान गर्न सकिने जानकारीहरू समावेश गर्ने डेटा सुरक्षा र गोपनीयता घटनाहरूलाई तेस्रो-पक्ष ठेकेदारले कसरी व्यवस्थापन गर्नेछ भनेर निर्दिष्ट गर्नुहोस्;

७. यदि, कसरी र कहिले डाटा डिस्ट्रिक्टमा फर्काइनेछ, उत्तराधिकारी ठेकेदारमा ट्रान्जिसन, जिल्लाको निर्देशनमा, तेस्रो-पक्ष ठेकेदारद्वारा मेटाइयो वा नष्ट हुन्छ जब सम्झौता समाप्त हुन्छ वा समाप्त हुन्छ वर्णन गर्नुहोस् ।

अन्तर-सन्दर्भ: स्कूल जिल्ला रेकर्ड (११२०)
मिडिया सम्बन्ध (११३०)
प्रतिबन्धात्मक सदस्यता वा कानून द्वारा अधिकृत र अनुमति दीएको रोजगार अभ्यास संग संगठनहरु द्वारा भर्ती (१२४०.१)
इन्टरनेट नीति (४५२६)

सन्दर्भ: राज्य प्रविधि कानून §§२०१-२०८
श्रम कानून §२०३-डि

नोटहरू: संकल्प नं. २०१०-११: ९०६ बमोजिम जुन २२, २०११ ग्रहण गरिएको; संशोधन नम्बर २०१८-१९: ८० अनुसार जुलाई २६, २०१८; २०२२-२३: २०६ को संकल्प नं. अनुसार २० अक्टोबर २०२२ मा संशोधित

सि.टि