jamf

Konformität im Bildungswesen für Einsteiger

Wie man einen Konformitätsplan für Schulen entwickelt, der Schüler, Lehrer und Gemeinden schützt

Die moderne Konformitätslandschaft im Bildungswesen

In jeder Branche kann die Konformität von Geräten und Netzwerken eine komplexe Angelegenheit sein. Die Branchenstandards ändern sich, wenn sich die Funktionen der Geräte erweitern – und wenn sich Gesetze oder bewährte Verfahren wandeln.

In Lernumgebungen verschlimmert sich diese Komplexität.

Sie erfahren:

- **Wie man mit den sich ständig ändernden Anforderungen an die Konformität im Bildungswesen Schritt halten kann**
- **Warum ein strategischer Ansatz für die Konformitätsinfrastruktur wichtig ist**
- **Wie man nachhaltige Konformitätspraktiken aufbaut**

Dieses Dokument dient nur zu Informationszwecken und stellt keine Rechtsberatung dar. Die Anforderungen an die Konformität variieren je nach Rechtsprechung und Institution. Schulen und Bezirke sollten sich an einen geeigneten Rechtsbeistand wenden, um ihre spezifischen Konformitätsverpflichtungen zu ermitteln.

Einzigartige Herausforderungen bei der Konformität in Schulen

Genau wie Unternehmen müssen auch Schulen die Vielzahl der Geräte und Benutzer, die sich mit den Schulnetzwerken verbinden, schützen und vor Cyberangriffen schützen.

Im Gegensatz zu Unternehmen müssen Schulen jedoch eine sehr offene und einfache Kommunikation mit Eltern und der Öffentlichkeit ermöglichen – wobei alle Beteiligten Geräte nutzen, über die Ihr Schulbezirk keine Kontrolle hat.

Dadurch entsteht eine große Angriffsfläche. Nimmt man die Budgetbeschränkungen hinzu, mit denen viele Schulen und Bezirke zu kämpfen haben, wird deutlich, dass die Einhaltung von Sicherheitsvorschriften eine ständige Herausforderung darstellt.

Die Benutzer der Geräte und der Netzwerke in Schulen sind ebenfalls klar identifizierbar.

Der größte Unterschied zwischen Unternehmen und Schulen besteht darin, dass Schulen eine wahrhaft enorme Vielfalt an Benutzern haben, darunter Lehrkräfte und Admins, Mitarbeiter der Schule und des Schulbezirks sowie – was vielleicht die größte Herausforderung darstellt – Kinder.

Kinder sind neugierig. Kinder brauchen ansprechende, interaktive Lernmittel. Sie müssen sich die Fähigkeiten aneignen, die sie brauchen, um verantwortungsbewusste digitale Bürger zu werden, und sie müssen das, was sie gelernt haben, mit ihren Lehrern, Familien und Gleichaltrigen teilen.

Die Neugierde von Kindern ist grenzenlos.

Deshalb muss die IT-Abteilung der Schule ihnen gewisse Grenzen setzen. Ihre Aufgabe: Kinder vor Phishing-Versuchen, Malware und gefährlichen oder ungeeigneten Inhalten zu schützen - ohne das tägliche Lernen und Lehren zu beeinträchtigen.

Darüber hinaus müssen die Schulen ein Gleichgewicht zwischen Cybersicherheitspraktiken und der Privatsphäre der Schüler herstellen. Und für einige der schwächsten Schüler, wie z. B. LGBTQIA+-Kinder, kann die Verletzung ihrer Privatsphäre extrem gefährlich für ihre psychische Gesundheit und körperliche Sicherheit sein.

Sich überschneidende Normen und Anforderungen

Das Bildungswesen steht weltweit unter strenger Beobachtung und enormem Druck aus verschiedenen Richtungen:

1. **Nationale und internationale Rechtsvorschriften**
2. **Regionale Gesetze und Normen**
3. **Bildungsaufsichtsbehörden**

In der EU schützt zum Beispiel die Allgemeine Datenschutz-Grundverordnung (DSGVO) die Daten von Schülern und Studenten, im Vereinigten Königreich sind es die UK General Data Protection Regulation (UK GDPR) und der Data Protection Act 2018. Auch kinderspezifische Gesetze und Vorschriften kommen zur Anwendung, wie z. B. das US-Gesetz zum Schutz von Kindern im Internet.

Darüber hinaus gibt es in Schulen häufig Anforderungen, die sich auf die Sicherheit von Daten, Netzwerken und Geräten auswirken können, wie z. B. das US-Gesetz für Menschen mit Behinderungen (Americans with Disabilities Act).

Und vergessen Sie nicht die Behörden, die die Einhaltung von Sicherheitsstandards zertifizieren, die Schulen erfüllen möchten, wie beispielsweise StateRAMP und FedRAMP – zwei Sicherheitsebenen, die häufig von staatlichen Organisationen verlangt werden, mit denen Schulen zusammenarbeiten möchten.

Die Herausforderung der digitalen Transformation

In den Klassenzimmern der 12. Klassen auf der ganzen Welt hat sich fast über Nacht ein enormer Wandel vollzogen, der sowohl durch die Corona-Pandemie als auch durch die verstärkte Konzentration auf die Sicherheit in Schulen ausgelöst wurde.

Schulen, die eine digitale Transformation durchlaufen, nehmen folgende Änderungen vor:

- **Umstellung von papiergestützten auf digitale Lernumgebungen**
- **Erhöhte Anforderungen an die Erhebung und Speicherung von Daten**
- **Fernunterricht und hybrides Lernen und deren Folgen für die Konformität**

Gemeinsame Konformitätsthemen in verschiedenen Rahmenwerken

Neben diesen zahlreichen Unterschieden in Bezug auf die Einhaltung von Vorschriften zwischen Schulen und Schulbezirken einerseits und Unternehmen andererseits müssen Schulen zudem Anforderungen und bewährte Verfahren in folgenden Bereichen einhalten:

- Datenschutz und Schutz der Privatsphäre
- Sicherheit von Geräten und Netzwerken
- Zugangskontrolle und Authentifizierung
- Reaktion auf Vorfälle und Meldung von Sicherheitsverletzungen
- Prüfpfade und Berichterstattung

Cyberangriffe auf Schulen sind weit verbreitet

Leider sind Schulen und Gemeinden ein attraktives Ziel für Cyberkriminelle.

Die Daten, über die Schulen verfügen, einschließlich Sozialversicherungsnummern und anderer Identifikationsmerkmale, sind lukrativ. Außerdem speichern einige Schulbezirke die Kreditkarten der Eltern für Schulessen und Schulgebühren - das ist schnelles Geld.

Dies ist ein weitverbreitetes Phänomen: In der britischen Umfrage zu Cybersicherheitsverletzungen aus dem Jahr 2025 stellten 44 % der Grundschulen und 60 % der weiterführenden Schulen in diesem Jahr Verstöße oder Angriffe fest.

Die Kosten der Nichteinhaltung von Vorschriften

Viele Schulen und Bezirke haben einen hohen Preis dafür bezahlt. Einige wurden gezwungen, Lösegeld zu zahlen, andere wurden von Eltern wegen offengelegter Daten verklagt, wieder andere gerieten in die Schlagzeilen, weil sie nicht in der Lage waren, ihre Netzwerke und Daten zu schützen oder Verstöße ordnungsgemäß zu melden.

Finanzielle Sanktionen und rechtliche Konsequenzen

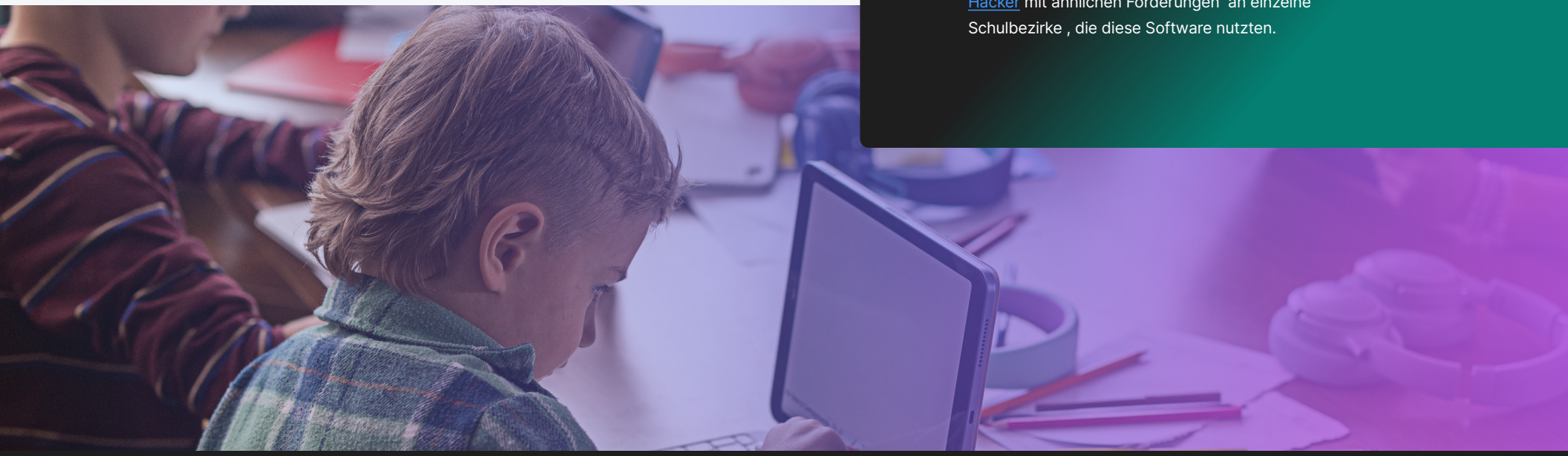
Wie bereits erwähnt, sind Schulen, Bezirke und sogar Anbieter, die sich nicht an strenge Sicherheits- und Datenschutzrichtlinien halten, in finanzielle und rechtliche Schwierigkeiten geraten.

Sie müssen exorbitante Lösegelder zahlen, verstoßen gegen nationale oder internationale Datenschutzgesetze für Schüler und werden von Eltern verklagt.

Ein kürzlich erfolgter Angriff auf einen Anbieter

Im Jahr 2024 hat ein weit verbreitetes Schülerinformationssystem (SIS) und eine Bildungstechnologieplattform 2,85 Millionen US-Dollar Lösegeld an einen Hacker gezahlt, der damit drohte, Schülerdaten offenzulegen, falls die Zahlung nicht erfolgte.

Schon im nächsten Jahr wandte sich derselbe Hacker mit ähnlichen Forderungen an einzelne Schulbezirke , die diese Software nutzten.



Rufschädigung und Verlust des Vertrauens in der Gemeinschaft

Schulen können das Vertrauen von Geldgebern, Eltern und lokalen Unternehmen verlieren, vor allem wenn sie keine klaren Regeln haben, wie sie die Öffentlichkeit über Verstöße informieren.

Ein kürzlich erfolgter Angriff auf einen Bezirk

Nach einem Ransomware-Angriff im Jahr 2023 informierte ein städtischer US-Schulbezirk die Öffentlichkeit nicht darüber, dass die Hacker Lösegeld verlangten und mit der Freigabe äußerst sensibler Daten drohten, falls die Zahlung nicht geleistet werden würde. Der Bezirk hat nicht gezahlt, und die Informationen wurden geleakt. Selbst nach der Offenlegung warteten sie monatelang, bis sie die betroffenen Schüler benachrichtigten. Die öffentliche Empörung hat dem Ruf des Bezirks geschadet.

Lehrkräfte achten auf die Wahrung der Privatsphäre ihrer Schüler, aber ohne klare Richtlinien können Schulen und Schulbezirke in eine schwierige Lage geraten, da sie aus verschiedenen Richtungen unterschiedliche und manchmal widersprüchliche Ratschläge erhalten. Wenn Schulbeamte nicht konsequent handeln, nimmt die Öffentlichkeit oft das Schlimmste an.

Betriebsunterbrechungen und Ressourcenzuweisung

Das ultimative Ziel von Cyberangriffen mag sicherlich der Profit sein, aber die Art und Weise, wie sie durchgeführt werden, kann Schulsysteme auf vielfältige Weise lahmlegen und zu Problemen führen:

- **Verzögerungen bei der Auszahlung von Gehaltsschecks**
- **Verspätete Zeugnisse**
- **Vollständige Schließung von Schulen für mehrere Tage**

Eine kürzlich geschlossene Schule

Im Januar 2026 musste eine weiterführende Schule im Vereinigten Königreich aufgrund eines Cyberangriffs eine Woche lang komplett geschlossen werden. Die Angreifer hatten „das gesamte IT-System der Schule lahmgelegt, einschließlich Telefon, E-Mail, Google Classroom, Schulverwaltungssysteme und Microsoft SharePoint“.

Da Sie diese Risiken nun kennen, sollten wir uns die grundlegenden Bestandteile ansehen, die einen soliden Plan zur Konformität ausmachen.

Vier zentrale Säulen der Konformität im Schulwesen

Schutz der Schülerdaten

Was sind Schülerdaten?

Das Verständnis darüber, was Schülerdaten (oder auch Daten von Lehrkräften oder Eltern) ausmacht, ist der erste Schritt zur Erstellung von Richtlinien und Verfahren zum Schutz dieser Daten. Diese Daten umfassen unter anderem, sind jedoch nicht beschränkt auf:

- Namen, Geburtstage, Anschriften und persönliche E-Mail-Adressen
- Namen, Informationen zum Arbeitsort und Kreditkartennummern der Eltern
- Daten wie Testergebnisse und Noten
- Aufzeichnungen über Gesundheit, Verhalten und Anwesenheit

Grundsätze der Datenminimierung

Die Minimierung der gesammelten Daten und deren Aufbewahrungsdauer kann viel dazu beitragen, die Privatsphäre der Schüler zu schützen. Erheben Sie nur Daten, die für den Betrieb zwingend erforderlich sind, und speichern Sie diese nur für die Dauer der Notwendigkeit. Hacker können nicht auf Informationen zugreifen, die nicht vorhanden sind.

Erlauben Sie nur denjenigen, die sie tatsächlich benötigen, den Zugriff auf die von ihnen benötigten Daten. Ein begrenzter Zugang schafft eine kleinere Angriffsfläche.

Legen Sie Zustimmungs- und Benachrichtigungsanforderungen fest. Stellen Sie sicher, dass Sie transparent kommunizieren, welche Daten Sie anfordern und warum, sowie wo und wie lange sie gespeichert werden. Dadurch entsteht Vertrauen in der Gemeinde.

Verwalten Sie Ihre Drittanbieter umfassend, wie z. B. Unternehmen für Test- oder Lernsoftware**.** Überprüfen Sie, ob die Anbieter die Sicherheits- und Datenschutzprotokolle einhalten. Legen Sie Richtlinien und Arbeitsabläufe fest, um sicherzustellen, dass Sie genau wissen, auf welche Daten Sie ihnen Zugriff gestatten, wie sie verwendet werden und was die Anbieter mit diesen Daten tun werden. Auf diese Weise wird die häufigste Angriffsform verhindert: Sicherheitsvorfälle bei Drittparteien.

Vier zentrale Säulen der Konformität im Schulwesen

2.

Grundlagen der Zugriffsverwaltung

Rollenbasierte Zugriffsprinzipien

Wie bereits erwähnt, ist es von entscheidender Bedeutung, den Zugang zu Netzwerken und Daten so zu verwalten, dass eine Person so wenig Zugang wie möglich benötigt: Geben Sie ihr das, was sie für ihre Arbeit benötigt, und nicht mehr. Stellen Sie sich immer folgende Frage: Wer sollte wann Zugriff auf was haben?

Durchsetzung rollenbasierter Zugriffsrechte

Stellen Sie sicher, dass Sie eine Möglichkeit haben, die Zugriffsrechte für Mitarbeiter zu erweitern, wann und wo dies benötigt wird – und dass der Zugriff für Gäste und Besucher auf das notwendige Minimum (Least Privilege) beschränkt wird. Dies lässt sich oft am besten kontrollieren, wenn diese Berechtigungen mit Schüler-, Eltern- und Lehrer-IDs verknüpft sind.

Altersabhängige Flexibilität

Denken Sie daran, dass die Anforderungen an den Zugang und die Authentifizierung je nach Rolle und Alter variieren können. Jüngere Lernende können sich möglicherweise keine komplexen Passwörter merken, während ältere Schüler dies schon eher können. Und natürlich ändert sich mit dem Alter der Schüler auch ihr Zugang aufgrund von neuen Lehrplänen. Die Zuweisung von klassen- oder altersabhängigen Rollen für die Schüler kann Ihnen auf lange Sicht viel Ärger ersparen.

Vier zentrale Säulen der Konformität im Schulwesen

3.

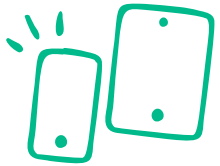
Anforderungen an die Sicherheitsinfrastruktur

Die Festlegung klarer Anforderungen an die Sicherheitsinfrastruktur und der Einsatz energischer Endpunktschutzstrategien können den Unterschied zwischen einem teilweisen und einem vollständigen Verstoß, zwischen einem gefährdeten und einem sicheren Gerät ausmachen.

Strategien zum Schutz von Endgeräten

Stellen Sie sicher, dass Sie über einen Endpunktschutz verfügen, der Folgendes bietet:

- Automatisierte Bedrohungsabwehr und Behebung
- Analyse auf dem Gerät und proaktive Berichterstattung
- Automatisierte Durchsetzung von Datenrichtlinien



Genauso entscheidend wie der Funktionsumfang ist die Gewährleistung, dass die Implementierung Ihrer Lösung weder die Sicherheit noch den Datenschutz oder die Performance beeinträchtigt.

Überlegungen zur Segmentierung des Netzwerks

Eine der besten Methoden, um zu verhindern, dass sich ein teilweiser Verstoß zu einem bezirksweiten Verstoß ausweitet, ist die Segmentierung Ihrer Netzwerke auf der Grundlage der Personen, die das Netzwerk nutzen, oder den Abteilungen, denen das Netzwerk dient. Sie können z. B. Admin- und Lehrernetzwerke, Schülernetzwerke und Gastnetzwerke haben.

Fortsetzung...

Vier zentrale Säulen der Konformität im Schulwesen

3. Anforderungen andie Sicherheitsinfrastruktur

Verschlüsselungsstandards und Implementierung

Schauen Sie sich genau an, welche Verschlüsselungs- und Implementierungsstrategien die verschiedenen Aufsichtsbehörden verlangen - und welche bewährten Verfahren Sie anwenden können:

- Starke Verschlüsselungsalgorithmen
- Sichere Schlüsselverwaltung
- Verschlüsselung der Daten bei Speicherung und Übermittlung

Regelmäßige Sicherheitsbewertungen

Da sich die Schülerpopulationen verändern und die IT-Tools weiterentwickelt werden, müssen Sie sicherstellen, dass Sie regelmäßig Sicherheitsbewertungen durchführen. Diese Sicherheitsprüfungen sind für eine kontinuierliche Konformität absolut unerlässlich.

Dies gibt Ihnen die Möglichkeit:

- neue und aufkommende Technologien zu implementieren
- Richtlinien zur Erfüllung aller Änderungen interner oder externer Konformitätsanforderungen und bewährter Verfahren zu entwickeln
- zu prüfen, ob es Lücken im Berichtswesen gibt oder ob neue Berichte erforderlich sind
- Ihre Anbieter und deren Eignung für neue oder erweiterte Anforderungen zu bewerten

Vier zentrale Säulen der Konformität im Schulwesen

4. Dokumentation und Prüfungsvorbereitung

Die Vorbereitung auf Audits mag wie eine lästige Pflicht erscheinen. Die richtige Vorbereitung auf Audits kann Ihnen jedoch nicht nur langfristig Zeit sparen, wenn Audits anstehen, sondern auch die Sicherheit Ihrer Netzwerke und Daten erhöhen.

So klappt es mit dem Audit:

Wesentliche Datenkategorien für die Verwaltung und Berichterstattung

Denken Sie an die drei großen Gruppen von Daten, die Sie tracken müssen:

Schülerdaten der: Anwesenheit, Noten und Verhaltensaufzeichnungen
Betriebliche Daten: Berichte über den IT-Bestand, Netzwerkkonfigurationen und Sicherheitsprotokolle
Rechtliche Daten: Konformitätsdokumente, Lieferantenverträge und Prüfberichte

Grundlegende Verfahren zur Dokumentation und Aufzeichnung

Stellen Sie sicher, dass Sie sichere, zentralisierte und konforme Daten verwalten. Zu den wichtigsten Praktiken gehören:

Verwendung eines Schülerinformationssystems (SIS)

Verwaltung des Hardware-/Softwarebestands

Digitalisieren von Unterlagen, wenn und wo es angebracht ist

Fortsetzung...

Vier zentrale Säulen der Konformität im Schulwesen

4. Dokumentation und Auditvorbereitung

Automatisierte Protokollierung und Überwachung

Audits sind viel einfacher, wenn Sie bereits über eine Praxis zur automatischen Erfassung, Analyse und Verarbeitung von Sicherheitsprotokolldaten in Echtzeit verfügen. Sie verfügen dann nicht nur über stets aktuelle Listen, sondern können auch proaktiv Sicherheitsbedrohungen erkennen und beseitigen, bevor sie sich zu echten Angriffen entwickeln.

Verfahren zur Dokumentation von Vorfällen

Vermeiden Sie Misstrauen innerhalb und außerhalb Ihrer Schule, indem Sie bereits festgelegte Dokumentationsverfahren für den Fall bereithalten, dass – und nicht ob – es zu einem Sicherheitsvorfall kommt. Stellen Sie sicher, dass Sie über Verfahren zur Dokumentation und Präsentation folgender Aspekte verfügen:

- Eine lückenlose, chronologische Darstellung des Vorfalls sowie der zur Ereignisbewältigung eingesetzten Werkzeuge
- Eine Bewertung der sicherheitstechnischen, betrieblichen und finanziellen Auswirkungen
- Ein Bericht über Befehlsausgaben, Protokolldateien und betroffene Systeme

Regelmäßige Überprüfung der Konformität

Genau wie bei den regelmäßigen Sicherheitsbewertungen ist auch dieser Prozess unerlässlich. Die Instrumente und Anforderungen zur Einhaltung von Richtlinien entwickeln sich ebenso kontinuierlich weiter wie Best Practices. Wer Zeit und Personal für die regelmäßige Überprüfung der Konformität bereitstellt, kann gesetzliche Strafen, Geldbußen und eine dauerhafte Rufschädigung verhindern.

BEWERTUNG DER KONFORMITÄTSBEREITSCHAFT

Sind Sie bereit?

Eine Checkliste zur Selbsteinschätzung

Dieser sich ständig weiterentwickelnde, strenge und komplexe Prozess kann mitunter überfordernd wirken. Deshalb sind Checklisten eine hervorragende Methode zur Vorbereitung, damit Ihrem Team nichts entgeht.

BEREITSCHAFT DER TECHNOLOGISCHEN INFRASTRUKTUR

Verfügen Sie über diese Elemente?

- [ ] Ein System zur Inventarisierung und Verwaltung von Geräten
- [ ] Zentralisierte Identitäts- und Zugriffsverwaltung
- [ ] Netzwerksegmentierung zwischen Schüler- und Verwaltungssystemen
- [ ] Endpunktschutz für alle Geräte
- [ ] Verschlüsselung von Daten im Ruhezustand und bei der Übertragung
- [ ] Automatisierte Sicherungs- und Wiederherstellungsprozesse
- [ ] Funktionen zur Sicherheitsüberwachung und Alarmierung

OPERATIVE BEREITSCHAFT

Sie sollten diese Komponenten implementieren:

- [ ] Ernennung eines Compliance-Beauftragten oder eines entsprechenden Teams
- [ ] Durchführung regelmäßiger Sicherheitsbewertungen
- [ ] Funktionen für Audit-Trails
- [ ] Etablierte Verfahren zur Meldung von Verstößen
- [ ] Festlegung von Kommunikationsprozessen für Eltern und Schüler
- [ ] Systeme zur Dokumentation und Aufzeichnung

PRÜFUNG DER RICHTLINIEN- UND GOVERNANCE-KONFORMITÄT

Sie sollten folgende Aspekte dokumentiert oder festgelegt haben:

- [ ] Umfassende Richtlinien zur akzeptablen Nutzung
- [ ] Maßnahmen zur Aufbewahrung und Entsorgung von Daten
- [ ] Verfahren zur Reaktion auf Vorfälle
- [ ] Schulungsprogramme für das Personal
- [ ] Lieferantenmanagement und Due-Diligence-Prozesse
- [ ] Ein Zeitplan für die regelmäßige Überprüfung und Aktualisierung der Richtlinien

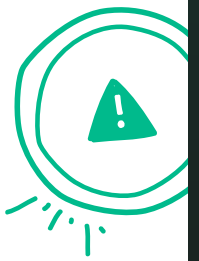
BEREITSCHAFT VON ANBIETERN UND DRITTEN

Haben Sie die folgenden Maßnahmen ergriffen?

- [ ] Datenverarbeitungsverträge mit allen Anbietern
- [ ] Ein Verfahren zur Überprüfung der Sicherheitszertifizierung
- [ ] Regelmäßige Sicherheitsbewertungen der Anbieter
- [ ] Klare Kontrollen bei der Weitergabe von und für den Zugriff auf Daten
- [ ] Anforderungen an die Vorfallsmeldungen durch Drittanbieter

Wie Jamf for K-12 die Konformität unterstützt

Obwohl Jamf for K-12 die Compliance Ihrer Schule nicht selbst automatisiert oder garantiert, bietet es die essenzielle Infrastruktur zur Unterstützung Ihrer gesamten Konformitätsstrategie durch:



Geräteverwaltung und Sicherheit:

- Zentralisierte Geräteregistrierung und -konfiguration
- Automatisierte Durchsetzung von Sicherheitsrichtlinien
- Verwaltung und Schutz der Geräte aus der Ferne
- Umfassende Bestandsaufnahme und Berichterstattung über Geräte

Zugriffskontrolle und Authentifizierung:

- Integration vont Identitätsdiensten für Single Sign-on (SSO)
- Rollenbasierte Zugriffsverwaltung
- Rollenbasierte Einschränkungen für Apps und Inhalte
- Sichere Authentifizierung über Geräte und Plattformen hinweg

Skalierbare Verwaltung:

- Konsistente Anwendung von Richtlinien auf allen Geräten
- Effiziente Verwaltung großer Geräteflotten
- Skalierbare Richtlinienbereitstellung für große Geräteflotten
- Unterstützung für unterschiedliche Lernumgebungen (Einzelgeräte, gemeinsam genutzte Geräte, BYOD)

Fähigkeiten zur Integration

- Funktioniert mit bestehenden Schulinformationssystemen
- Unterstützt Bildungsapps von Drittanbietern
- Integration in die Netzwerkinfrastruktur
- Konnektivität mit Lösungen für die Identitäts- und Zugriffsverwaltung

Die Jamf-Plattform dient als Fundament, das den Bezirken hilft, die zuverlässige, sichere und verwaltbare Technologieumgebung aufzubauen, die für die Konformität erforderlich ist.

Unsere Automatisierungen und Funktionen ermöglichen es Ihrem Team, sich auf Richtlinien, Schulungen und strategische Konformitätsinitiativen zu konzentrieren, anstatt sich mit den täglichen Herausforderungen der Geräteverwaltung aufzuhalten.

Compliance in Schulen ist nie abgeschlossen.

Es handelt sich um einen kontinuierlichen Prozess, der sich mit Ihrer Technologie, Ihrer Schülerpopulation und dem rechtlichen Umfeld weiterentwickelt.

Die gute Nachricht ist, dass Sie diese Grundlage nicht allein aufbauen müssen.

Jamf for K-12 gibt Ihrem Team die Werkzeuge an die Hand, um Geräte zu verwalten, Richtlinien durchzusetzen und die Art von sicherer, überprüfbarer Umgebung aufrechtzuerhalten, die die Konformität erfordert. Das bedeutet weniger Zeitaufwand für die Infrastruktur und mehr Zeit für die Arbeit, die wirklich wichtig ist.

Kostenlose Testversion anfordern

jamf