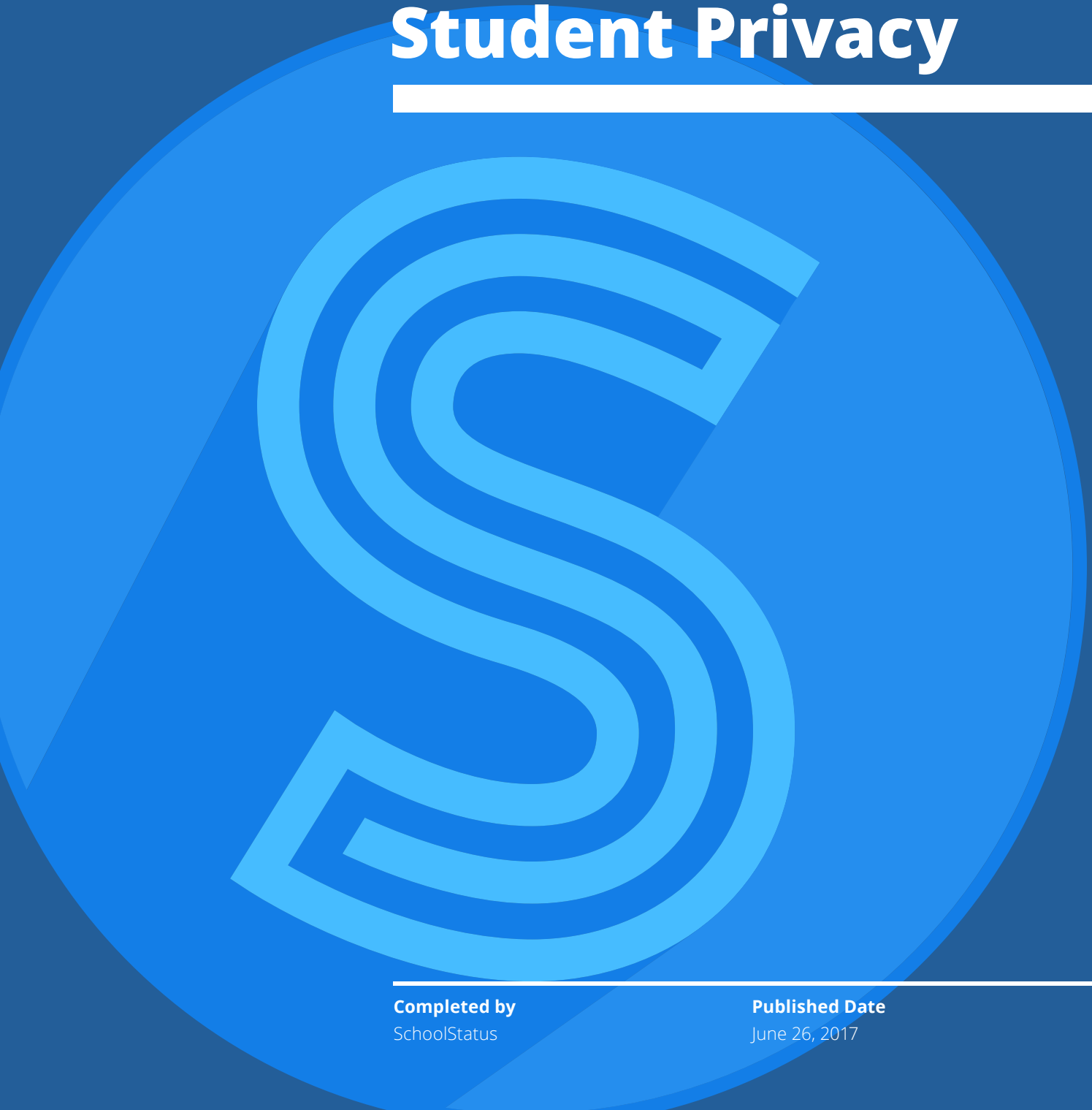
SchoolStatus

The Importance of Data Security when it comes to Student Privacy



Completed by
SchoolStatus

Published Date
June 26, 2017

01 Corporate Policies and Procedures

About Us

- *SchoolStatus* exclusively employs and contracts with people who abide by certain legal requirements as outlined by our legal risk team.
- All employees and contractors are required to agree to and sign strict data confidentiality contracts that deal with the privacy and handling of *SchoolStatus'* and, more importantly, our customers' data.
- When *SchoolStatus* hires new employees, they are required to submit to a federal and state-level criminal background investigation in addition to a check against the child abuse registry. Additionally, for employees with relevant professional licenses (i.e.: Certified Public Accountants or Teachers) to ensure those licenses are active and have no disqualifying disciplinary history.

Employee Single Sign-On

- Our human resource information system (HRIS) is linked to our employee credential system to ensure that employees who are terminated immediately lose access to all *SchoolStatus* digital resources.
    - We also employ single sign-on using a centralized directory with application entitlements. This ensures when a user's *SchoolStatus* account is terminated, they lose access to all other electronic resources (including e-mail) immediately.
    - Our single sign-on system also requires the use of two-factor authentication, which requires not only a password to login to electronic resources, but also a complex, rotating key that is time based.
- All workstations and mobile devices at *SchoolStatus* utilize whole disk encryption which helps prevent data from being gleaned from laptops or mobile devices that may have been stolen or otherwise compromised.
- *SchoolStatus* provides ongoing training and source code reviews to ensure customer data is kept in the most secure method possible for the use-case.

Need To Know Basis

- Most importantly, customer data is kept on a need-to-know basis. This means that customer data is not allowed to be possessed or accessed by those who don't need it for their jobs.

Example An executive assistant may come in contact with data in a limited capacity during the normal course of duty for their job. They may see a teacher's name mentioned in a technical support e-mail… but they wouldn't be able to access a customer's parent contact information because their day-to-day responsibilities don't necessitate it.

- In addition to restricting data on a need-to-know basis, we routinely employ a least-liability model with regards to data access.

Example We restrict access to production data to a few who may need it to do their job. A junior programmer working on developing a part of our software would be provisioned an anonymized version of data as opposed to live access to customer data. One could argue access to live data would be required for their job, but it is a better risk mitigation practice that they use anonymized data instead.

Manual Data Transmission

We do not accept non-public personal identifiable information via e-mail or other non-secure channel. If a customer sends a file via e-mail (a very common but dangerous practice), we immediately purge the file and ask that they use our secure upload site instead. **NO EMAIL. NO WAY.**

(Is this cat image copyrighted?)

We never accept email traffic serving attachments without transport-layer (TLS) encryption. This helps prevents the sending of potentially sensitive data over insecure methods.

02 Physical Security

A surprising amount of data loss occurs through a commercial burglary setting or various breakdowns in physical security (i.e. non-shredding of sensitive information resulting in data loss). *SchoolStatus* discourages our customers from sending data in a physical medium if at all possible, and only houses PII on its physical premises when required by our customers (for instance, when a customer sends data to us on Compact Disc format). Once we complete the upload of the PII to a secure storage medium, we destroy the data in question using a secure methodology (shredding the Compact Disc, in our example) or return it to the customer using a secure trackable courier service. While data is housed locally, (at one of our two Mississippi locations before it is returned to the customer) we store it in a secure locked safe.

Again, we discourage our customers from sending data in a physical medium if at all possible.

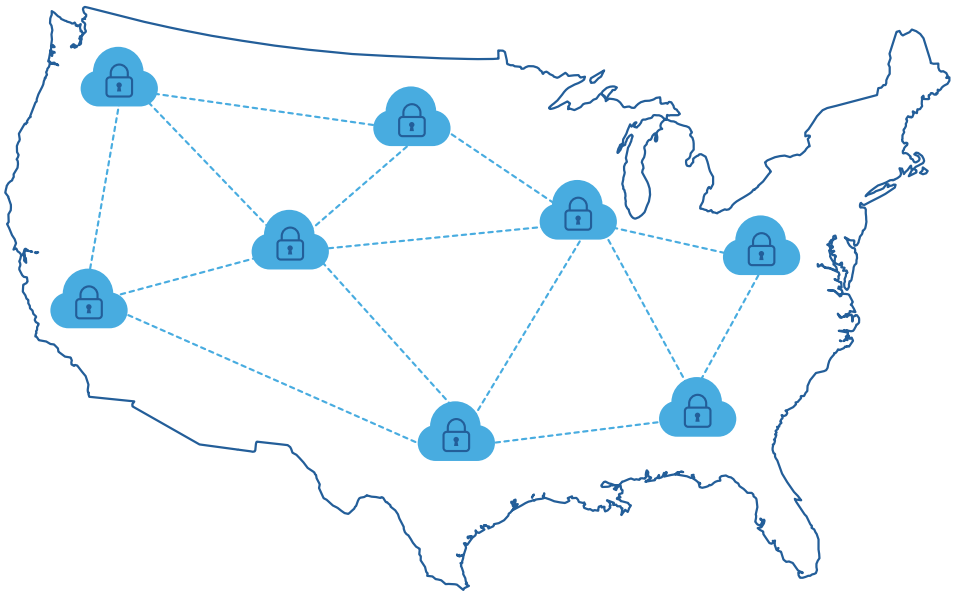
Physical Location Access

Access to our physical work locations requires a physical badge token that is unique to each employee and is not easy duplicated. This allows for us to restrict physical access to our work locations immediately upon employee termination and ensure only those individuals needing access to our work locations have access.

We do not routinely utilize removable storage (such as flash/USB drives) to intentionally prevent their loss or theft.

03 Data Architecture and Storage Security, including Cloud Hosting

SchoolStatus uses a cloud-based Platform as a Service (PaaS) provider. Doing so allows us to innovate and keep the costs of our services low for our customers. By using our PaaS provider, *SchoolStatus* isn't forced to build and maintain expensive telecommunications infrastructure and undergo the expense of maintaining a data center. By leveraging the tools and capabilities our PaaS provider furnishes us, we're able to maintain geographic diversity (to avoid Earthquakes, Tornados, or other disasters from making our service unavailable) and essentially unlimited scaling capabilities (so we can add customers quickly and efficiently).



Our configuration and legal agreement with our PaaS provider allows for the following:

- Data that is stored within *SchoolStatus* never leaves the United States and is never available to other companies. Our data is logically and physically separate from other companies running in the same data center.
- Because all datastores and files are configured to be encrypted at rest, it's mathematically improbable that a 3rd party would be able to read them if they compromised the physical hardware on which our software runs.

Compliance with Certifications, Privacy Laws, and Legal Frameworks

Certifications	Privacy Laws	Legal Treaties & Frameworks
DoD SRG	FERPA	CIS
FedRAMP	GLBA	CJIS
FIPS	HIPPA	CLIA
ISO 9001	HITECH	CMS EDGE
ISO 27001	IRS 1075	CMSR
ISO 27017	ITAR	CSA
ISO 27018		EU-US Privacy Shield
PCI DSS Level 1		FISC
SEC Rule 17-a-4(f)		FISMA
SOC 1		GxP (FDA CFR 21 Part 11)
SOC 2		ICREA
SOC 3		MITA 3.0
		MPAA
		NIST
		PHR
		Uptime Institute Tiers

Geographic Redundancy

SchoolStatus operates in multiple regions across the United States. Regions are designed for availability and consist of at least two, often more, Availability Zones. Availability Zones are designed for fault isolation. They are connected to multiple Internet Service Providers (ISP's) and different power grids. They are interconnected using high-speed links, so applications can rely on local area network (LAN) connectivity for communication between Availability Zones within the same region.

SchoolStatus operates in two geographically diverse Regions, each having at least four availability zones. It is unlikely, but not impossible, that a natural disaster should render all of them unavailable. For this reason, we fully backup and snapshot our encrypted customer data to a geographically diverse storage network that boasts a 99.999999999% object durability. For example, if you store 10,000 backup objects, we can on average expect to incur a loss of a single object once every 10,000,000 years. Bottom line: it's highly unlikely physical permanent data loss of customer data will occur.

Visual Suggestion Imagine a timeline or evolution-type visual showing the following playful analogy - "If you store 10,000 backup objects, you could actually build a time machine, travel back in time, hang out with Mr. T-Rex, and we still wouldn't have lost any of your data. It's that secure." (PS - Can Mr. T-Rex please wear a Top Hat?) :)

03 Data Architecture and Storage Security, including Cloud Hosting

Shared Tenancy Controls

For purposes of economy of scale, most modern Software as a Service (SaaS) applications employ a multi-tenancy model - just as your school's banking institution doesn't operate a separate branch location and server devoted to just your school. Without this, SaaS applications would become too expensive to develop, maintain, and therefore use by schools. Instead of running our platform on a new server for each customer, we run them on shared resources. We provide logical software controls to keep your data from being available to non-authorized individuals.

SchoolStatus' products have been architected to provide logical separation using global non-repeating 128-bit identifiers assigned to each district and school. These are used to determine data ownership for every data point stored with us. When a user logs into our platform, we set a user's scope to allow access on a primary level to, and only to, their district's data as delineated by their 128-bit identifier. This occurs at the data store level so that even if a user were to be able to compromise our code base, they would still be unable to access another district's data as a result.

Remote Server Access

Direct access to our servers requires a secure virtual private network (VPN client) and rotating secure shell (SSH) keys. Server passwords are disabled, only SSH key access is allowed. Remote access is restricted to staff members with an absolute and demonstrable need for requiring such access. Remote server administration isn't available to the public internet as only SSL/TLS traffic is exposed through a load balancer. Access rules and routing rules are in place to prevent access to the servers that run our application except through traffic load balancers. All other access is prevented.

Our application and database servers are logically separated into their own private container and layer 2 network. All traffic inbound and outbound is tightly controlled through a defined set of rules to defined destinations. Servers which serve internal functions and aren't serving up public SSL traffic are generally not allowed to access the public internet.

Logging

In addition to logging who and to which students our end-users access, we also log all servers to a central location in a read-only fashion. There is no capacity to alter or delete a log entry once it has been made. All SSH, VPN, remote access, and other system events are monitored for anomalies. Server access logs are saved for at least one year; end-user logs are saved in perpetuity.

Two-Factor Authentication

In addition to traditional usernames and complex passwords, administrative access to our software and system requires a second security credential. This credential is a long integer that rotates every 30 seconds based upon a complex algorithm

outlined in RFC 6238[1]. Brute force guessing this credential is unlikely and requires a specific piece of software and code that is only available to each of our staff members, typically stored on a mobile phone. This process provides assurance that even if a staff member's password is compromised, dubious 3RD parties are unable to access our systems without also having access to a user's mobile phone. Likewise, having access to just their mobile phone without the user's password is equally as useless.

All *SchoolStatus* information systems, including e-mail, also use two-factor authentication in the same manner.

[1] *https://en.wikipedia.org/wiki/Time-based_One-time_Password_Algorithm*

Antivirus and Anti-Malware and Software Updates

All *SchoolStatus* workstations, servers, and other systems are protected by antivirus and antimalware services. System state of these services is closely monitored and turning off this capacity is very difficult and time consuming, by design. Servers that have their antivirus and anti-malware capabilities turned off are alerted to almost immediately to prevent remote-access software from being installed surreptitiously.

Staff workstations and devices that do not have active antivirus and antimalware running are automatically barred from accessing our corporate wireless access network and company resources.

Software updates are automatically applied and are monitored for compliance on regular schedule. Servers are routinely updated to the latest server and software components to patch against known software vulnerabilities.