t. 044 500 10 90
e. info@escola.ch
w. www.escola.ch

a. Escola GmbH
Beckenhofstrasse 72
8006 Zürich

Technische und organisatorische Massnahmen der Escola GmbH

Mit diesem Dokument informieren wir Sie über die getroffenen technischen und organisatorischen Massnahmen, welche zur Gewährleistung der Sicherheit von personenbezogenen Daten getätigt werden. Das Hosting der Kundensysteme erfolgt nicht in den Räumlichkeiten von Escola, sondern wird an Unterauftragnehmer ausgelagert. Durch den Abschluss von Auftragsdatenberarbeitungs-Vereinbarungen mit dem Unterauftragnehmer werden die dazugehörigen technischen und organisatorischen Massnahmen für das Rechenzentrum gewährleistet.

Verantwortliche:	Escola GmbH Beckenhofstrasse 72 8006 Zürich
Datenschutzverantwortlicher:	Hannes Bärtschi
IT-Verantwortlicher:	Janick Pfenninger
Datum:	28.10.2024

Inhalt:

t. 044 500 10 90
e. info@escola.ch
w. www.escola.ch

a. Escola GmbH
Beckenhofstrasse 72
8006 Zürich

1 Massnahmen zur Sicherheit interner Systeme

1.1 Zugangskontrolle

1.1.1 Einsatz einer Firewall zum Schutz der Netzwerke.
1.1.2 Sicherung der Computer von Mitarbeitenden mittels passwortgeschützter Zugänge.
1.1.3 Automatische Sperrung der Computer der Mitarbeitenden nach einer bestimmten Inaktivitätszeit.
1.1.4 Verwendung individueller Passwörter zur Vermeidung von Gruppen-Passwörtern.
1.1.5 Multi-Faktor-Authentifizierung für alle internen Informationssysteme.
1.1.6 Nutzung eines Passwortmanagers zur sicheren Verwaltung von Passwörtern.
1.1.7 Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitenden.
1.1.8 Prozess zum Rechteentzug bei Abteilungswechseln von Mitarbeitenden.
1.1.9 Prozess zum Rechteentzug bei Austritt von Mitarbeitenden.
1.1.10 Spam-Filter im E-Mail-System der Mitarbeitenden.
1.1.11 Vergabe eindeutiger Kennungen für alle Nutzer.

1.2 Vertraulichkeit

1.2.1 Beschränkung der Berechtigungen der Mitarbeitenden auf das erforderliche Minimum.
1.2.2 Nutzung einer sicheren Übertragungsmethode für den Austausch von sensiblen Daten zwischen Auftraggeberin, Auftragnehmerin und Dritten.
1.2.3 Verwendung von Aktenvernichtern gemäss DIN 66399 zur Vernichtung sensibler Dokumente.

2 Massnahmen zur Sicherheit der Kundensysteme

2.1 Zutrittskontrolle zum Rechenzentrum

2.1.1 Zugangsberechtigungskonzept unter Einbeziehung von Berechtigungslisten.
Der Zugang zu den Rechenzentren ist nach schriftlicher Voranmeldung per E-Mail und in Begleitung eines Mitarbeitenden des Service-Anbieters möglich.
2.1.2 Einsatz von Sicherheitsschleusen
2.1.3 Zugangskontrolle zum Rechenzentrum mittels Videokontrolle, Key-Card und persönlichem PIN-Code.
2.1.4 Physische Schutzmassnahmen zur frühzeitigen Erkennung einer Verletzung des Perimeters.
2.1.5 Die Server des Service-Anbieters befinden sich in zwei voneinander getrennten Tier 3 Rechenzentren im Kanton Freiburg in der Schweiz.

- Rechenzentrum I: Bonnstrasse 20, CH-3186 Düdingen
- Rechenzentrum II: Duensstrasse 1, CH-3186 Düdingen

Beide Standorte verfügen über eine unterbrechungsfreie Stromversorgung, Dieselstromaggregate und Notstrombatterie-Anlagen, Präzisionsklimasysteme, ein Frühwarnalarmsystem und eine Brandmeldeanlage.

2.2 Authentifizierung

2.2.1 Login Timeouts (Throttling): Automatische Sperrung von Nutzeraccounts für 5 Minuten nach zehnfacher Fehleingabe von Passwörtern. Alle Fehleingaben werden geloggt.
2.2.2 Protokollierung aller Zugriffe auf die Kundensysteme.
2.2.3 Zwei-Faktor-Authentifizierung bei Support-Zugriffen auf die Kundensysteme.

2.2.4 Die Leistungsbezügerin kann selbst über den Einsatz von Zwei-Faktor-Authentifizierung je Benutzergruppe entscheiden.
2.2.5 Vorgabe einer allgemeinen Mindestkomplexität von Passwörtern, zusätzlich können Administratoren die Mindestkomplexität von Passwörtern je Nutzergruppe erhöhen (Password Policy).
2.2.6 Beim ersten Login ist die Änderung des Initialpasswortes erforderlich.
2.2.7 Zeitverzögerung zwischen einzelnen Login-Versuchen.

2.3 Autorisierung

2.3.1 Der Datenzugriff erfolgt unter Berücksichtigung festgelegter Autorisierungsregeln entsprechend den jeweiligen Nutzer-Rollen.
2.3.2 Einschränkung der Zugriffsberechtigung der Mitarbeitenden auf Kundendaten auf das erforderliche Mass.
2.3.3 Möglichkeit zur Zuweisung unterschiedlicher Superuser für verschiedene Bereiche der Software.

2.4 Kryptographie

2.4.1 Speicherung von Passwörtern ausschliesslich in verschlüsselter Form (Hash einschliesslich Salt-Wert) in der Datenbank.
2.4.2 Verschlüsselung aller Datenbank-Backups.
2.4.3 Verschlüsselung aller Festplatten (Encryption at rest)
2.4.4 Ausschliessliche Verwendung verschlüsselter HTTPS-Verbindungen (TLS) zu den Kundensystemen (Encryption in Transit). Schlüssel: Es werden jeweils die aktuellsten Let's Encrypt-Standards verwendet.
2.4.5 Ausschliesslich verschlüsselte Verbindungen (HTTPS / SFTP (TLS/SSL)) zu Drittsystemen bei Import- und Export-Schnittstellen (Encryption in Transit).

2.5 Integrität

2.5.1 Protokollierung von Datenlöschungen auf Anweisung der Leistungsbezügerin.
2.5.2 Möglichkeit zur autonomen Datenlöschung bestimmter Bereiche durch die Leistungsbezügerin.
Die Leistungsbezügerin kann definieren, welche Bereiche (beispielsweise Journal, Dossier, Zeugnisse) nach einer definierten Zeitspanne gelöscht werden sollen.
2.5.3 Umfassende Datenlöschung auf Anfrage der Leistungsbezügerin.
2.5.4 Vollständige Datenlöschung bei Kündigung des Vertrages.
Solid State Disk (SSD): Die Informationen auf dem Gerät werden gelöscht, indem die Flash-Zellen als leer markiert werden.
Festplatte (HD): Die Informationen werden geschreddert und mit einem Strom von Bytes mit Nullwerten überschrieben.
Wechseldatenträger: Die Informationen werden geschreddert und mit einem Strom von Bytes mit Nullwerten überschrieben.
Zusätzlich zu diesen Massnahmen sind alle Speichermedien verschlüsselt (encryption at rest, s. Kapitel 2.4.3).
2.5.5 Trennung der Kunden durch ein Einzelmandantensystem.
Die Daten sowie die Datenbank einer Schule werden getrennt von anderen Schulen gehalten. Pro Kunde gibt es dedizierte, virtuelle Instanzen.
2.5.6 Sperrung externer Inhalte durch eine dynamische Content Security Policy.
2.5.7 Time-Sync: Alle Systeme sind zeitlich synchronisiert und loggen mit dem gleichen Zeitstempel (Stratum 2), dabei kann die Zeitzone durch den Kunden selbstständig definiert werden.
2.5.8 Logs (Audit Trail): Alle Logins und relevanten User-Aktionen (wie beispielsweise Mutationen an Stammdaten, Anstellungen, Massnahmen uvm.) werden detailliert

t. 044 500 10 90
e. info@escola.ch
w. www.escola.ch

a. Escola GmbH
Beckenhofstrasse 72
8006 Zürich

geloggt. Ebenso werden alle API-Zugriffe von Umsystemen protokolliert. Die Daten werden ohne zeitliche Begrenzung gespeichert.

2.5.9 Alle Daten werden als Objekte in logischen Speicherpools (CEPH) gespeichert. Die Daten werden mit Replica 3 gespeichert. Die Daten werden auf Ceph bluestore gespeichert, dadurch werden bei allen Schreibvorgängen crc32c-Prüfsummen erzeugt. Die Prüfsummen wird bei jedem Lesen von Daten getestet. Wird ein Fehler festgestellt, werden die Daten automatisch von einem anderen Replikat abgerufen. Die Replikate werden in regelmässigen Abständen verglichen, um die Daten weiter vor Korruption zu schützen und Probleme frühzeitig zu erkennen. Einzelheiten finden Sie in der Dokumentation hier: https://www.ibm.com/docs/en/storage-ceph/7?topic=components-data-integrity

Backups: Die Daten werden mit Kopia gesichert: https://kopia.io/
Die Backups werden in einem anderen Ceph-Pool gespeichert als der VM-Blockspeicher. Mithilfe von S3-Aufbewahrungsrichtlinien werden Backups für eine bestimmte Zeit nach ihrer Erstellung vor Löschung oder Manipulation geschützt (s. 2.7.3).

2.6 Entwicklung, Release-Regeln und Prinzipien

2.6.1 Durchführung von Funktionalitätstests, Leistungstests, Regressionstests und Code-Reviews vor Software-Updates.

2.6.2 Festlegung von Datenbank-, Daten- und Code-Zugriffsrechten der Mitarbeitenden nach dem Prinzip der Bedarfsnotwendigkeit.

2.6.3 Trennung von Entwicklungs-, Test- und Produktivsystemen.

2.6.4 Entwicklung nach dem Grundsatz «Privacy by Design».

2.6.5 Keine personenbezogenen Daten im Source Code.

2.6.6 Keine API-Keys von Drittanbietern im Source Code.

2.6.7 Nutzung eines Key Vaults:
Alle API-Keys von Drittanbietern sind in einem spezialisierten Key Vault gespeichert; jede Anpassung und jeder Zugriff auf Keys durch Mitarbeitende wird aufgezeichnet, nur ein beschränkter Personenkreis hat Zugriff auf die Keys und Keys können jederzeit zurückgenommen / ersetzt werden (Key-Revocation). TLS-Zertifikate werden via Certbot generiert und auf dem Server der Schule gelagert. Es existiert ein Salt und Pepper für jegliche Passwörter.

2.6.8 Regelmässige Durchführung von Penetrationstests durch externe Dienstleister.
Escola führt regelmässige Blackbox-Penetrationstest durch, dabei werden alle relevanten Komponenten des Systems (Backend, API, Web- und Mobile-App) getestet. Zusätzlich werden ereignisgesteuerte Whitebox-Pentests bei sensitiven Änderungen oder für neue Produkte durchgeführt. Penetrationstests werden von unterschiedlichen Dienstleistern durchgeführt. Seit 2023 ist unser externer Dienstleister Code Purple. Anbei finden Sie eine Auswahl der letzten Tests, die durchgeführt wurden.

Whitebox-Review Passkeys 2024
Durchführungsperiode: Oktober 2024
Bestätigung und Inhaltsverzeichnis: https://dateien.escola.ch/tom/Whitebox-TestLogin Passkey 2024 - Bestätigung und Inhaltsverzeichnis.pdf [Link]

Whitebox-Test Login OAuth 2024
Durchführungsperiode: Januar 2024
Bestätigung und Inhaltsverzeichnis: https://dateien.escola.ch/tom/Whitebox-TestLogin OAuth 2024 - Bestätigung und Inhaltsverzeichnis.pdf [Link]

Penetrationstest 2023

Durchführungsperiode: April – Mai 2023
Bestätigung und Inhaltsverzeichnis: https://dateien.escola.ch/tom/Penetrationstest 2023 - Bestätigung und Inhaltsverzeichnis.pdf [Link]

2.6.9 Escola verwendet eine Web Application Firewall (WAF).

2.6.10 Für die Application Security werden unter anderem die OWASP-Top-10 beachtet.

2.7 Verfügbarkeit

2.7.1 Jede Stunde werden Backups aller Datenbanken und Daten gemacht. Das Backup wird mittels Kopia per Push-Backup auf einem Server der Stepping Stone gespeichert. Das Backup wird bei der Erstellung verschlüsselt. Der Server ist S3-kompatibel und Ransomware-protected (S3 Object Lock).
Parallel dazu wird ein zweites Backup erstellt, das bei Infomaniak (Serverstandort: Schweiz) verschlüsselt gespeichert wird.

2.7.2 Datenbank-Backups werden verschlüsselt auf den Servern von Unterauftragnehmern gespeichert.

2.7.3 Für Daten- und Datenbank-Backups gelten folgende Aufbewahrungszeiten:
7 Tage: ein Backup pro Stunde
90 Tage: ein Backup pro Tag
52 Wochen: ein Backup pro Woche
3 Jahre: ein Backup pro Monat

2.7.4 Prozess zur Wiederherstellung des Gesamtsystems oder der Rekonstruktion von Daten
RPO s. 2.7.3, Wiederherstellungsdauer (RTO) des Gesamtsystems von einer Stunde ab Erkennung des Incidents: www.escola.ch/isms#imp

2.7.5 Regelmässige Überprüfung der Datensicherung in Testroutinen.

2.7.6 Periodische Tests von Backup-Wiederherstellungen zur Gewährleistung der Funktionalität.

2.7.7 Brand-, Rauch- und Feuchtigkeitsmeldeanlagen im Rechenzentrum

2.7.8 Redundante Stromversorgungen und die notwendigen Systeme, um einen autarken Betrieb des Rechenzentrums für einen definierten Zeitraum zu ermöglichen

2.7.9 Einsatz eines Stromgenerators bei Stromausfällen im Rechenzentrum

2.7.10 Redundant verteilte Datenträger im Rechenzentrum

2.7.11 Redundante Netzwerke im Rechenzentrum

2.7.12 Geofencing: Zugriffe aus bestimmten Regionen können akzeptiert (whitelist) oder blockiert (blacklist) werden.
Spezifische Anforderungen von Kunden sind via OpenStack Security Groups (Firewall Regeln) umsetzbar: https://docs.openstack.org/nova/latest/user/security-groups.html

2.7.13 Alle betriebenen Systeme werden nach Schadsoftware überprüft.
Security Patches werden monatlich in den geplanten Wartungsfenstern eingespielt. Alle Systeme sind so weit wie möglich gehärtet. Für die Linux-basierten Systeme wird SELinux1 (Security-Enhanced Linux) eingesetzt. Es wird eine regelmässige Risikobeurteilung durchgeführt und die daraus abgeleiteten Massnahmen werden umgesetzt. Um die Sicherheit der Infrastruktur zu gewährleisten, müssen sicherheitsrelevante Patches zeitnah eingespielt werden können. Dazu dienen ungeplante Wartungsarbeiten, welche zeitnah und nach Möglichkeit ausserhalb der regulären Arbeitszeiten durchgeführt werden. Die Ankündigung von ungeplanten Wartungsarbeiten erfolgt via Information im Escola Portal sowie via E-Mail und so frühzeitig wie möglich.

2.7.14 Der physikalische Aufbau der Cloud-Infrastruktur basiert auf zwei redundanten und geografisch voneinander getrennten Rechenzentren.
Das Besondere an dieser Architektur ist, dass beide Rechenzentren aktiv genutzt werden. Alle Daten werden in beiden Rechenzentren gespeichert. Die Übertragung erfolgt – unabhängig vom Internet – über 2x 100 Gigabit/s

Vollduplex-Glasfaser-Verbindungen. Dies ermöglicht es, eine virtuelle Maschine vom Rechenzentrum Bonnstrasse ohne Unterbruch ins Rechenzentrum Duensstrasse zu migrieren. Sollte es zu einem Ausfall eines der beiden Rechenzentren kommen, können die ausgefallen Maschinen innerhalb von wenigen Minuten manuell neu gestartet werden. Sobald das ausgefallene Rechenzentrum wieder zur Verfügung steht, können die virtuellen Maschinen wieder auf beide Standorte verteilt werden. Die Netzwerkinfrastruktur ist ebenfalls redundant aufgebaut. Es sind mehrere Uplinkprovider angeschlossen, sodass bei einem Ausfall eines Uplinkproviders die Cloud-Infrastruktur über andere verfügbare Verbindungen erreichbar bleibt. Alle Komponenten der Cloud-Infrastruktur sind redundant ausgelegt. Die nachfolgende Grafik zeigt den physikalisches Aufbau dieser Infrastruktur auf:
https://dateien.escola.ch/tom/Infrastruktur_Aufbau.jpg

2.7.15 Die virtuellen Maschinen laufen auf der redundanten Cloud-Infrastruktur.
https://dateien.escola.ch/tom/Virtuelle_Infrastruktur.jpg

2.7.16 Redundanz
Die Redundanz der virtuellen Server erfolgt auf Filesystem-Ebene mit Ceph2 (ein hoch skalierbares, verteiltes Dateisystem). Die Daten werden auf jeweils drei verschiedenen Solid State Disks (SSDs) basierten Storage-Nodes gespeichert. Die virtuellen Server werden mit der Kernel-based Virtual Machine3 (KVM) Technologie virtualisiert. Eine virtuelle Maschine kann im laufenden Betrieb ohne Ausfall von einer Compute-Node auf eine andere migriert werden. Daher führen Wartungsfenster der Basis-Infrastruktur nicht zu Ausfällen der virtuellen Maschinen. Kommt es doch einmal unerwartet zu einem Ausfall einer Compute-Node, so werden die darauf laufenden VMs direkt nach dem Neustart der Compute-Node auch wieder hochgefahren. Im Fall einer beschädigten Compute-Node, die sich nicht mehr starten lässt, können die virtuellen Maschinen auf einer anderen Compute-Node neu gestartet werden.

2.7.17 Firewall
Jede virtuelle Maschine wird durch eine iptables4-basierte Firewall auf der Compute-Node (dem Trägersystem der virtuellen Maschinen) lokalisierte Firewall geschützt. Standardmässig sind alle Ports (incoming und outgoing) gesperrt. Die benötigten Ports werden gezielt geöffnet. Die Firewall-Regeln lassen sich aus einer virtuellen Maschine heraus nicht manipulieren. Bei der Migration einer virtuellen Maschine von einer Compute-Node zu einer anderen Compute-Node werden die Firewall-Regeln ebenfalls migriert.

3 Kontrollverfahren

3.1.1 Meldung neuer oder veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten.

3.1.2 Prozesse zur Meldung neuer oder veränderter Verfahren sind dokumentiert.

3.1.3 Getroffene Sicherheitsmassnahmen werden einer regelmässigen internen Kontrolle unterzogen.

3.1.4 Es besteht ein Incident-Response-Prozess für Vorfälle. Details s. www.escola.ch/isms#imp

3.1.5 Einsatz von Softwarelösungen zur Unterstützung des Datenschutz-Managements.

3.1.6 Alle Server-Hoster sind ISO27001-zertifiziert.

3.1.7 Sofortige Einbindung der Auftragsverantwortlichen bei Sicherheitsvorfällen und Datenpannen.

3.1.8 Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeitende nach Bedarf und Berechtigung.

t. 044 500 10 90
e. info@escola.ch
w. www.escola.ch

a. Escola GmbH
Beckenhofstrasse 72
8006 Zürich

3.1.9 Zentrale Erfassung sämtlicher vorhandener Dienstleister, Auftragsverarbeiter und Unterauftragnehmer.

4 Management und Organisation

4.1.1 Zentrale Erfassung vorhandener Dienstleister, Auftragsverarbeiter und Unterauftragnehmer.
4.1.2 Abschluss einer Auftragsdatenbearbeitungs-Vereinbarung mit den Server-Anbietern.
4.1.3 Regelmässige interne Kommunikation, einschliesslich Bereitstellung von Updates zur Software und relevanten Betriebsinformationen.
4.1.4 Regelmässige Sensibilisierung und Schulung der Mitarbeitenden.
4.1.5 Verschwiegenheitsklausel als integraler Bestandteil der Arbeitsverträge mit den Mitarbeitenden.