SWOP.

Die Software.

eine Software der

SmartKomm GmbH

Informationsblatt Sicherheit & Datenschutz

Stand Juni 2024

Grundlegende Sicherheits-Funktionsweise 2
Sicherheitsmechanismen 2
Benutzer, Berechtigungen und Passwörtern 3
Benutzer-Accounts 3
Passwörter 3
Berechtigungen 3
Sicherheit in der Datenübertragung 3
Sicherheitsvorkehrungen innerhalb der Softwarentwicklung 3
Sicherheits-Merkmale des Server-Hostings 4
Verschlüsselte und verteilte Backups 4
Datenschutz 4
a) Vertraulichkeit 4
b) Integrität 6
c) Verfügbarkeit 6
d) Authentizität 6
e) Revisionsfähigkeit 7
f) Transparenz 7

Grundlegende Sicherheits-Funktionsweise

- Lehrer dürfen alle Daten lesen. Lehrer dürfen an ausgewählten Stellen Informationen eintragen. Lehrer können keine Zugriffsberechtigungen ändern oder einstellen.

- Schüler dürfen grundsätzlich nur Ihre eigenen persönlichen Daten lesen, sowie natürlich auf öffentliche und Klassenzug-bezogene Daten zugreifen. Schüler können keine Daten von Mitschülern einsehen.

- Eltern dürfen grundsätzlich nur die persönlichen Daten ihrer Kinder lesen, sowie auf öffentliche und Klassenzug-bezogene Daten zugreifen. Eltern können keine Daten von anderer Schüler oder Eltern einsehen.

- Schulfremde haben keinerlei Zugriff auf internen Bereiche.

- Nur geschultes Personal mit entsprechender Berechtigung darf Rechte vergeben und Sicherheitseinstellungen verändern.

Sicherheitsmechanismen

SWOP ist mit einem flexiblen und einfach zu bedienenden Sicherheits-System ausgestattet.

Jeder einzelnen Seite werden sogenannte ACLs (Access-Control-Lists) zugeordnet, die für genau diese eine Seite festlegen, welche Gruppe und welcher Benutzer die hier dargebotenen Informationen lesen darf und wer diese Daten verändern darf.

Absichtlich wurde auf Vererbung, automatische oder anderweitig implizite Rechte verzichtet, um ungewollte Rechteweitergabe zu verhindern.

Grundsätzlich dürfen Seiten oder Bereiche im SWOP von niemandem eingesehen werden, außer es wird explizit durch eine entsprechend autorisierte Person dieses Recht durch eine ACL auf der betreffenden Seite erstellt.

Ausschließlich entsprechend geschultes und über datenschutzrechtliche Grundlagen aufgeklärtes Personal soll Berechtigungen verändern. Nur entsprechend geschulten und datenschutzrechtlich aufgeklärten Lehrern wird die zum Einstellen von Rechten notwendige Berechtigung erteilt.

Benutzer, Berechtigungen und Passwörtern

Benutzer-Accounts

Einen Zugang SWOP erhalten nur offiziell mit der Schule assoziierte Personen, definierte Administratoren und ggf. Mitarbeiter der SmartKomm GmbH.

Passwörter

Alle Passwörter werden per Zufallsgenerator erstellt und Lehrern, Eltern und Schülern in gedruckter Form persönlich überreicht, oder per Post zugeschickt. Jeder Nutzer kann jederzeit sein Passwort selbst verändern. Eine strenge Passwort-Komplexitäts-Richtlinie sorgt dafür, dass das neu vergebene Passwörter wieder sicher sind.

Berechtigungen

Nur entsprechend geschulten und datenschutzrechtlich aufgeklärten Personen wird die Möglichkeit eingeräumt, Berechtigungen zu verändern oder zu erstellen.

Sicherheit in der Datenübertragung

Alle sensitiven Daten werden ausnahmslos über Ende-zu-Ende SSL verschlüsselte Internet-Verbindungen übertragen. Sollte versucht werden, Daten unverschlüsselt abzurufen, so bricht das Schul - Webportal bereits vor der Übertragung die Verbindung ab.

Sicherheitsvorkehrungen innerhalb der Softwarentwicklung

Die SmartKomm GmbH verwendet modernste und ausgereifte Mechanismen zur regelmäßigen Funktions- und Sicherheits-Testung des Schul - Webportals nach aktuellem Stand der Technik.
Neben Black-Box, Gray-Box und White-Box Testing-Verfahren werden auch manuelle Code-Audits, Security- Reviews und viele verschiedene automatische Testverfahren angewendet. Durch stetiges Updaten des zugrunde liegenden Software-Frameworks auf die jeweils neuesten Versionen wird sichergestellt, dass stets die neuesten und aktuellsten Sicherheits-Techniken benutzt werden.

Sicherheits-Merkmale des Server-Hostings

Die dedizierten Server von SWOP steht in zwei modernen Rechenzentren in den Räumen eins deutschen Hostingpartners. Mit diesem Partner hat die SmartKomm GmbH ein besonderes Datensicherheitskonzept und eine eigene vertragliche Übereinkunft zur Datenverarbeitung im Auftrag im Einklang mit § 3 Abs. 1 Bundesdatenschutzgesetz und den landesdatenschutzrechtlichen Vorschriften zur Auftragsdatenverarbeitung geschlossen.

Das Rechenzentrum ist 24/7 durch Wachpersonal besetzt. Zusätzlich werden alle sensiblen Bereiche durch Kameras überwacht. Damit sich keine Unbefugten in der Nähe Ihrer Server aufhalten können, sorgt ein modernes Zugangskontrollsystem dafür, dass nur autorisierte Personen Einlass erhalten.

Ein umfassendes Sicherheitskonzept garantiert, dass alle Daten im Rechenzentrum vor Diebstahl oder Beschädigung durch Umwelteinflüsse geschützt sind. Alle kritischen Werte in den Räumlichkeiten (Temperatur, Luftfeuchtigkeit, Stromversorgung usw.) werden von der Gebäudeleittechnik permanent überwacht.

Verschlüsselte und verteilte Backups

Die Sicherheit der Daten wird durch automatische tägliche Backups gewährleistet. Die Daten werden ausschließlich verschlüsselt gespeichert und werden automatisch auf unterschiedliche Standorte verteilt um selbst im Falle von z.B. Bränden oder Naturkatastrophen die sichere Lagerung aller Daten sicherzustellen.

Datenschutz

a) Vertraulichkeit

Maßnahmen, die bewirken, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können:

- Nur entsprechend geschulten und datenschutzrechtlich aufgeklärten Personen wird die Möglichkeit eingeräumt, Berechtigungen zu verändern oder zu erstellen.
- Grundsätzlich dürfen Module und Bereiche von niemandem eingesehen werden, außer es wird explizit durch eine entsprechend autorisierte Person dieses Recht erstellt.

- Alle Passwörter werden per Zufallsgenerator erstellt und Lehrern, Eltern und Schülern in gedruckter Form persönlich überreicht, oder per Post zugeschickt. Jeder Nutzer kann jederzeit sein Passwort selbst verändern. Eine strenge Passwort-Komplexitäts-Richtlinie sorgt dafür, dass die neu vergebenen Passwörter wieder sicher sind. Eine 2-Faktor-Authentifizierung ist vorgesehen.
- Einen Zugang zu Daten von SWOP erhalten nur die Schulleitung und Lehrer der Schule sowie ggf. Mitarbeiter der SmartKomm GmbH. Andere Personen erhalten grundsätzlich keinen Zugang, außer es liegt eine gesetzlich vorgeschriebene Ausnahme oder richterliche Verfügung vor.

- Default Rechtelage im SWOP
  - Lehrer dürfen alle Daten über Schüler lesen. Lehrer dürfen an ausgewählten Stellen Informationen eintragen. Lehrer können keine Zugriffsberechtigungen ändern oder einstellen.
  - Schüler dürfen grundsätzlich nur Ihre eigenen persönlichen Daten lesen, sowie natürlich auf öffentliche und Klassenzug-bezogene Daten zugreifen. Schüler können keine Daten von Mitschülern einsehen.
  - Eltern dürfen grundsätzlich nur die persönlichen Daten ihrer Kinder lesen, sowie auf öffentliche und Klassenzug-bezogene Daten zugreifen. Eltern können keine Daten anderer Schüler oder Eltern einsehen.
  - Schulfremde haben keinerlei Zugriff auf interne Bereiche.
  - Sonderrechte, z.B. für Klassensprecher oder Elternvertreter, können durch den Auftraggeber vergeben werden. Diese Sonderrechte sind jedoch nur für entsprechende abgetrennte und gekennzeichnete Veröffentlichung-Bereiche und nicht für die persönlichen Daten einzelner Schüler möglich.
- Alle sensitiven Daten werden ausnahmslos über Ende-zu-Ende SSL verschlüsselte Internet- Verbindungen übertragen. Sollte versucht werden, Daten unverschlüsselt abzurufen, so bricht SWOP die Übertragung ab.
- Alle Daten und Back-ups werden ausschließlich verschlüsselt gespeichert
- Daten eines Schülers werden nach dem Verlassen der Schule gelöscht.
- Schüler bzw. deren Erziehungsberechtigten haben ein Auskunftsrecht sowie ein Recht auf Berichtigung, Sperrung und Löschung gespeicherter Daten. Sofern einer Löschung gesetzliche oder vertragliche Aufbewahrungspflichten oder andere gesetzliche Gründe widersprechen, werden die Daten entsprechend gesetzlicher Vorgaben archiviert. Die digitalen Daten werden daraufhin aus dem SchulWebportal gelöscht.

b) Integrität

Maßnahmen, die bewirken, dass personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben:

- Alle Daten stehen immer im direkten gegenseitigen Zusammenhang zwischen Schule, Eltern und Schülern. Evtl. auftretende Fehler fallen schnell auf und werden entsprechend z.B. von Schülern dem Klassenlehrer oder von Eltern der Schulleitung gemeldet. Entsprechende Korrekturen können jederzeit durch Berechtigte vorgenommen werden
- Alle Änderungen werden durch ein Versionssystem protokolliert
- Entsprechend dem Stand der Technik werden aktuelle und moderne Softwaresysteme eingesetzt die die Integrität der Daten sicherstellen. Eingesetzt werden unter anderem Datenbank-Constraints, Foreign- Key Constraints, Daten-Validatoren, Dependent-Deletes, Transaction-Handling, Continuous-Testing, strenge Daten-Typisierung und spezialisierte Daten-Modellierung.
- Verwendung offener Standards garantiert eine identische und reproduzierbare Darstellung der Daten auch in Systemen unterschiedlicher Hersteller.
- Intelligente Eingabemasken unterstützen aktiv die Eingabe sinnvoller Daten und erschweren oder (wenn möglich) verhindern die Eingabe fehlerhafter Daten.

c) Verfügbarkeit

Maßnahmen, die bewirken, dass personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können:

- Aktive Betreuung des Systems mit einer vertraglich zugesicherten Verfügbarkeit von 99%.
- Einsatz von Monitoring-Software zur fortwährenden Überwachung aller Server-Systeme.

d) Authentizität

Maßnahmen, die bewirken, dass personenbezogene Daten jederzeit ihrem Ursprung zugeordnet werden können:

- Jedem Eintrag ist der Autor und das letzte Bearbeitungsdatum zugeordnet.
- Testergebnisse von Schultests können nur von dem Lehrer bearbeitet werden, der den Schultest in dem System angelegt hat.
- Metadaten können nur von dem Nutzer bearbeitet werden, der sie angelegt hat.

e) Revisionsfähigkeit

Protokollierungsverfahren, die die Feststellung erlauben, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat:

- Jedem Eintrag ist der Autor und das letzte Bearbeitungsdatum zugeordnet
- Noten können nur von dem Lehrer bearbeitet werden, der den Schultest in dem System angelegt hat.
- Metadaten zu Noten können nur von dem Lehrer bearbeitet werden, der den Schultest in dem System angelegt hat.
- Prinzipiell werden ausnahmslos alle Einträge in der SQL-Datenbank mit einem Erstellungs-Zeitstempel und einem Zuletzt-Bearbeitet-Zeitstempel versehen.
- Alle Aufträge zu Datenänderungen werden dem jeweiligen Auftraggeber schriftlich bestätigt und sind somit jederzeit nachvollziehbar.

f) Transparenz

(1) Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig und in zumutbarer Zeit nachvollzogen werden können:

- Alle Verarbeitungen personenbezogener Daten werden durch Menschen ausgeführt. eine automatisierte Verarbeitung findet nur in folgenden Fällen statt:
  - Eine automatisierte Durchschnittsberechnung von Noten je Schüler und je Schulfach wird durchgeführt. Die Berechnung wird vollständig und nachvollziehbar in einer entsprechenden Tabelle dargestellt.
- Jeder Eintrag kann jederzeit mit der Schulleitung oder einem Lehrer diskutiert werden.
- Dem Auskunftsbegehren nach DSGO, kann über entsprechende Reports in SWOP jederzeit stattgegeben werden
- Es stehen Dokumente zur Verfügung, die die verwendeten Verfahren erläutern.
- Ein umfassendes Benutzerhandbuch erläutert alle Verfahren.

(2) Die technischen Details der Umsetzung der Datensicherungsmaßnahmen sind Bestandteil des SWOP Vertragsschlussverfahrens

Dieses Dokument wurde

- **am 01.07.2011 erstellt,**
- **am 01.06.2024 letztmalig überarbeitet.**