FuxMedia GmbH & Co. KG · Karcherallee 25a · 01277 Dresden

Tel 0351·260 50 60
Fax 0351·260 50 94

Email info@fuxmedia.de
Web www.fuxmedia.de

HypoVereinsbank Dresden
Kto 357 954 274
BLZ 850 200 86
IBAN DE30 8502 0086 0357 9542 74
BIC HYVEDEMM496

FuxNoten®

1. Beschreibung der technischen Umsetzung:

FuxNoten - webbasierte Software zur Notenverwaltung

technische Details:

- Programmiersprache PHP
- PHP Version 5.5.30
- MySQL Version 5.6 Datenbank-System
- Apache/2.2.15 (CentOS)
- Arbeitsspeicher mindestens 128 MB
- Betriebssystem Linux oder Windows-WebServer

Funktionsumfang:

- Eingabe von Noten
- Import/Export von/zu FuxSchool, Indiware und anderer Software
- Drucken verschiedener Notenübersichten
- Verwaltung von Schülern, Lehrern, Klassen
- Bearbeitung von Wichtungen und Bereichen
- Elternzugänge anlegen und bearbeiten

2. Datensicherung:

- Backup Frequenz und Anzahl vom Administrator einstellbar
- können auf separatem System gespeichert werden

3. IT-Sicherheitskonzept:

Programmseitig existieren folgende Schutzmaßnahmen:

- Multiples Verschlüsselungs-System - jedes System verfügt über 3 einmalige Verschlüsselungs-Codes, somit können die Daten nicht ohne den passenden Code sowie des Verschlüsselungs-Algorythmus entschlüsselt werden
- Log-System mit eindeutiger Dokumentation von Zugriffen, Eingaben und Änderungen - inklusive IP für Rückverfolgung – somit elektronische Signatur der verwalteten Daten und Noten
- Möglichkeit der automatischen Benachrichtigung des Systembetreuers über Sicherheitsverstöße

- Automatisierte System/Nutzer/IP-Sperrungen konfigurierbar
- Elternportal - alle Zuordnungen, Nutzernamen, etc sind anonymisiert (werden durch den Nutzer bestimmt und können von der Schule nicht eingesehen werden)
- konfigurierbare Passwortrichtlinie
- Anpassung Namensdarstellung mit Möglichkeit der Kürzung des Vor-/Nachnamen
- SSL-Zertifikatsverschlüsselung
- 2-Faktor-Authentifizierung (TAN-Liste oder E-Mail TAN-Verfahren)
- Berechtigungskonzept (Benutzer/Rollen-System für zugeordnete Bereiche)

Desweiteren werden technische und organisatorische Datenschutzmaßnahmen der Auftragsdatenverarbeitung nach § 9 BDSG durchgeführt bzw. eingehalten.

Diese Anlage konkretisiert die Umsetzung der im Rahmen der Auftragsdatenverarbeitung erforderlichen technischen und organisatorischen Maßnahmen.

1. Zutrittskontrolle

Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird.

Es existieren folgende Maßnahmen zur Zutrittskontrolle:

- elektronisches transpondergesichertes Zutrittssystem
- schriftliche Betriebsanweisung für Schlüsselregelung für die Betriebsräume
- betriebsfremden Personen wird der Zugang zu den Betriebsräumen nur in Begleitung eines Mitarbeiters gewährt
- Einbruchmeldeanlage

2. Zugangskontrolle

Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird.

Es existieren folgende Maßnahmen zur Zugangskontrolle:

- serverseitige Laufwerksverschlüsselung
- Festlegung von individuellen Benutzerberechtigungen für jeden Mitarbeiter bzw. für Mitarbeitergruppen
- Einsatz einer Software-Firewall an jedem Arbeitsplatz
- vollständige Verschlüsselung von Datenträgern in Laptops/Notebooks

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf Daten zugreifen können, die ihrer Zugangsberechtigung unterliegen und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können.

Es existieren folgende Maßnahmen zur Zugriffskontrolle:

- Verwaltung der Rechte durch Systemadministrator
- Festlegung von Zugriffsberechtigungen für jeden Mitarbeiter
- Passwortrichtlinie inkl. Passwortlänge und Passwortwechsel
- Daten sind grundsätzlich servergespeichert, nicht lokal am Arbeitsplatz

4. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung solcher Daten im Datenverarbeitungssystem vorgesehen sind.

Es existieren folgende Maßnahmen zur Weitergabekontrolle:

- Verschlüsselung der Daten
- verschlüsselter Datentransport (HTTPS, SFTP, VPN)

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personen-bezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind.

Es existieren folgende Maßnahmen zur Eingabekontrolle:

- Eingaben sind nur nach explizierter Anmeldung möglich
- Protokollierung der Zugriffsberechtigten Bearbeiter
- Verfahrens- und Arbeitsanweisungen definiert

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Kundens verarbeitet werden können.

Im Regelbetrieb (keine Störung am System) greifen Mitarbeiter der FuxMedias nicht auf personen-bezogene Daten des Kundens zu. Störungen oder Fehlerkorrekturen können den Zugriff erforderlich machen. Störungen führen in der Regel, aber im Fall des Bedarfs von Datenveränderungen in jedem Fall zur Eröffnung eines Tickets in einem Ticket-System. Die Korrektur von fachlichen Fehlern durch Änderung von Dateninhalten wird ebenfalls durch Zuweisung eines Tickets in einem Ticket-System beauftragt. Tickets können per E-Mail, Telefon (0351-79998100) oder eine dafür zur Ver-fügung stehende Webplattform, erreichbar unter https://www.fuxmedia.de/anfragesystem/ vom Kunden erstellt werden. Im Ticket werden die ausgeführten Aktionen und Problemlösungen festgehalten.

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:

- gespiegelter Datenbestand
- täglicher Backup (Verwahrung des Datenträgers im Tresor)
- Einsatz von Schutzprogrammen (Virenscanner, Firewalls)
- Richtlinie zur Wartung und Durchführung von Updates

8. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Es existieren folgende Maßnahmen zur Verwendungszweckkontrolle:

- Kundentrennung - Daten werden in Kunden- und - auftragsspezifischen Verzeichnisse gespeichert
- getrennte Datenbanken