

SYSTEMANFORDERUNGEN

HSE-COACH und **HSE-MANAGER** sind browser- und datenbankbasierte Anwendungen zur Durchführung und Dokumentation von interaktiven Schulungen zu Arbeitsschutz und Arbeitssicherheit im Internet/ Intranet.

SYSTEMANFORDERUNGEN SERVER:

Server:	Single-CPU-System ab 1,5 GHz, 4GB RAM, ca. 20-100 GB Festplatte (abhängig von Inhalten)
Betriebssysteme:	beliebig; bevorzugt Windows, um Zusatzapplikationen realisieren zu können
Webserver:	Apache HTTP-Server aktuellste Version oder Alternative (Funktionsgarantie nur für Apache)
Mailserver:	SMTP anonymous oder user authentication. Optional nötig bei gewünschtem Versand von Prüfungsbestätigungen.
Skript:	PHP ab Version 5.6
Rechte:	voller RW-Zugriff auf Installationsverzeichnis und dessen Unterverzeichnisse; ggf. notwendige DB-Rechte Kunde
System-DB:	SQL-Datenbank (Funktionsgarantie nur für MySQL/MariaDB) andere DB-Typen erfordern ggf. kostenpflichtige Anpassungen
Interface-DB:	SQL-Datenbanken MySQL/MariaDB, MS-SQL oder andere DB per Web-Services (erfordern ggf. kostenpflichtige Anpassungen)

SYSTEMANFORDERUNGEN ARBEITSPLATZ/TERMINAL/TABLET:

System:	Single-CPU-System ab 1,5 GHz, 4GB RAM, ca. 10-20 GB Festplatte
Betriebssysteme:	Windows 10 Pro, Android, Linux, iOS mit Einschränkungen (ohne Video, da kein Autoplay und keine gekürzte Antwortsequenz möglich)
Browser:	Edge, Chrome, Firefox, Safari, Internet Explorer mit Einschränkungen
Rechte:	Wiedergabe vom mp3-/mp4-Dateien, RW-Zugriff per Script auf Installationsverzeichnis Server
Plugins:	keine Plugins notwendig, nur JavaScript muss aktiviert sein
Devices:	Lautsprecher oder Kopfhörer (empfohlen, sofern Audio- und/oder Video-Content) Touchscreen (dringend empfohlen für Systeme am Werkzeugzugang) Netzwerk-Peripherie bei Festverdrahtung ggf. (Karten-) Drucker ggf. Barcode-, QR-Code- oder Kartenlesegerät intern oder extern

STANDARD-PROTOKOLLE/PORTS:

FTP	TCP, Port 21
HTTPS	TCP, Port 443
NAS	TCP, Port 8081
Teamviewer	TCP/UDP, Port 5938

AUTHENTIFIKATIONS-METHODEN:

Standard:	Login mit User/Passwort-Kombination, die in der Regel je Installation einheitlich ist, d. h. per Default keine benutzerspezifische Passwort-Verwendung
ID-basiert	Erfassung einer beliebigen ID über manueller Eingabe oder Lesegerät (RFID, QR-Code, Barcode) und Abgleich mit einer Datenbank

STANDARD-SCHNITTSTELLEN / WEB-SERVICES:

Alle Schnittstellen werden mit 1 oder 2 Secret Keys gegen Missbrauch abgesichert.

- **hse-MANAGER: GetWorkerData (POST)**
User-Authentifikation per Web-Service (POST) zu hse-MANAGER.
- **Customer-Interface (POST)**
User-Authentifikation per Web-Service (POST) zu kundenspezifischem Web-Service.
- **Mail (POST)**
Optionaler Aufruf der internen E-Mail-Schnittstelle zum Versand der Prüfungsbestätigung (ggf. mit PDF-Anhang).
- **(S)FTP**
Erzeugt in einem definierten Remote-Verzeichnis eine CSV-Datei mit den kundenspezifischen Daten.
- **hse-MANAGER: InsertWorkerData (POST)**
Übergabe der personenbezogenen, neuen (!) User-Daten an Web-Service.
hse-MANAGER: UpdateWorkerData (POST)
Übergabe der personenbezogenen User-Daten an Web-Service zum Update vorhandener Daten.
- **hse-MANAGER: UploadWorkerFile (POST)**
Web-Service zum Upload personenbezogener Daten (Foto, Dokumente, Zertifikate, etc.).
- **Customer Interface (POST)**
Kundenspezifisch ausgeprägter Web-Service.