Sicherheits- und Datenschutzkonzept

eKompAss

Stand 01.09.2008

1 Technische Grundinformationen

1.1 Webhosting (Managed Webhosting)

Die Systemplattform wird auf einem angemieteten Platz (Colocation) in einem professionellem Rechenzentrum betrieben (gehostet). Die dort vorhandene Hardware ist jederzeit erweiterbar. Der Server wird als ein Managed Mietserver betrieben. Der Zugang zum System erfolgt nach Absprache. Der Betreiber des Rechenzentrums (Hoster) übernimmt das Aufsetzen der Betriebssystemumgebung, Wartung der Server, Monitoring, Firewalling, Backup und Managing der Server, z.B. Softwareupgrades und Updates bei Sicherheitslücken mit Sicherheitspatches.
(Die Beschreibung der technischen und räumlichen Infrastruktur finden Sie im Anhang)

1.2 Datenübertragung (Verschlüsselte SSL-Übertragung)

Das SSL-Protokoll gewährleistet, dass Daten während der Übertragung nicht gelesen oder manipuliert werden können und stellt die Identität einer Internetseite sicher.
Die Verschlüsselung des eKompAss-Systems erfolgt in der hohen Stufe (AES-256, 256 bit)

2 Passwortschutz

Der Zugriff auf das System durch Benutzer findet nach einer Anmeldung mit einem Benutzernamen und Passwort statt. Die Benutzer müssen davor von einer berechtigten Person innerhalb ihrer Bildungseinrichtung im System angelegt worden sein. Im Auslieferungszustand werden ausschließlich die vom Auftraggeber benannten Personen als Koordinatoren von MSO Mediatec GmbH eingetragen. Alle weiteren Benutzer sind dann vom Koordinator ein zu richten. Bei der Anlage von Benutzern werden auch der Benutzername und das Passwort vergeben. Ein Benutzername muss dabei auf das gesamte System bezogen eindeutig sein und der Aufbau des Passwortes muss bestimmten Regeln entsprechen (8 Zeichen, kleine und große Buchstaben, Zahlen und bestimmte Sonderzeichen. Erforderlich ist mindestens ein Sonderzeichen). Passwörter, die nicht diesen Regeln entsprechen werden vom System nicht angenommen. (Ab 01.10.2008)

Ein Benutzer im System kann sich im dem Zustand *aktiv* oder *inaktiv* befinden. Nur ein zum Zeitpunkt der Anmeldung am System aktiver Benutzer kann sich am System anmelden.
Der Aktivitätszustand kann von berechtigten Personen jederzeit geändert werden und dient vor allem dazu, Benutzer vom System auszuschließen bzw. ihnen wieder Zugang zu gewähren.

3 Benutzersitzung, Cookies

Das System setzt Benutzersitzungen ein. Eine Sitzung dauert 20 Minuten und wird automatisch beendet, falls ein Benutzer innerhalb dieser 20 Minuten keine Interaktion mit dem Serverrechner durchführt. Benutzersitzungen dienen der Sicherheit im Falle, dass ein Benutzer den Arbeitsplatz ohne Abmeldung vom System verlässt und es dadurch zum Missbrauch durch andere kommen könnte.
Ein weiterer Grund für den Einsatz von Benutzersitzungen ist, dass dadurch erst die Benutzer bestimmten Serveraktionen zugeordnet werden können und es dadurch zu einer zusammenhängenden Arbeit der einzelnen Benutzer kommen kann.
Für die Verfolgung der Benutzersitzungen werden Cookies eingesetzt (auf dem Client-Rechner gespeicherte kleine Datenpakete).

4 Protokollierung

Bei jedem Speichervorgang werden alle Aktionen protokolliert. (Vollprotokollierung)
Diese Log-Dateien werden separat in einer Datenbank gespeichert und sind nur vom Auftraggeber benannten Personen zugänglich. Die Log-Dateien werden gelöscht, wenn die entsprechenden personenbezogenen Daten gelöscht oder anonymisiert sind. (Ab 01.10.2008)

5 Gespeicherte Daten

5.1 Daten eines Benutzers:

- Name
- Vorname
- Username

- Passwort
- Telefon
- Email
- Diff-Id
- Notiz
- Aktiv
- Rolle

  (Die unterstrichenen Eigenschaften sind Pflichtangaben.)

5.2 Daten eines Teilnehmers:

- Name
- Vorname
- Kundennummer
- Geburtsdatum
- Straße
- Postleitzahl (PLZ)
- Ort
- Telefon
- Mobiltelefon
- Bildungsbegleiter
- Geschlecht
- Nationalität
- Schule
- Assessment

  (Alle Angaben sind optional.)

5.3 Daten eines Teilnehmer-Assessments (zugeordnet zu einem bestimmten Teilnehmer):

- Mikrobeobachtungen (freier Text, Häufigkeit des Vorkommens, zugeordnetes Kriterium)
- Notizen (frei formulierbar)
- Empfehlung (frei formulierbar)
- Hinweise (frei formulierbar)
- Selbsteinschätzung eines Teilnehmers

5.4 Daten eines Assessments:

- Name
- Kürzel
- Anfangsdatum
- Enddatum

  (Alle Angaben sind optional.)

6 Löschen der Daten

Nach Ablauf der vom Auftraggeber vorgegebenen Zeitspanne werden die Daten automatisch gelöscht oder anonymisiert. Eine Wiederherstellung der Daten nach dem Löschen oder eine Rückführung anonymisierter Daten in dem Ausgangszustand ist nicht möglich.

7 Verschiedene Bildungseinrichtungen

Mit einem Assessment-System können mehrere Bildungseinrichtungen arbeiten. Die Daten der einzelnen Bildungseinrichtungen sind dabei auf der Datenhaltungsebene logisch voneinander getrennt.

8 Rollenkonzept

Die Benutzer des Systems besitzen verschiedene Rollen.

8.1 Rollen im System:

A) Beobachter
B) Berichteschreiber
C) Verwaltung
D) Koordinator
E) Hauptkoordinator
F) Qualtitässicherung

Die Verwendung der Rollen erlaubt es, den Datenzugriff zu regeln indem den Rollen bzw. ihren Besitzern unterschiedliche Rechte zugesprochen werden.

Die Rollen sind hierarchisch verteilt, d.h. ein Benutzer mit der jeweils beschriebenen Rolle hat die beschriebenen Rechte und zusätzlich alle Rechte aller darunter liegenden Rollen.

	A)	B)	C)	D)	E)
Beobachter	X				
Berichteschreiber	X	X			
Verwaltung	X	X	X		
Koordinator	X	X	X	X	
Hauptkoordinator	X	X	X	X	X

Im Folgenden werden die einzelnen Benutzerrollen und die sich daraus ergebenden Rechte beschrieben.

8.2 A) Rechte der Beobachter:

Die teilnehmerbezogenen und teilnehmeraufgabenbezogenen Rechte gelten nur für die Teilnehmer, auf die der Benutzer Zugriff besitzt. Der Zugriff wird ihm dadurch erteilt, dass er Zugriff auf das Assessment erhält, in dem der Teilnehmer eingetragen ist!

- ✓ Lesender Zugriff auf Dokumente zu Grundinformationen des Verfahrens
- ✓ Lesender Zugriff auf Dokumentvorlagen zu Aufträgen
- ✓ Lesender Zugriff auf die Datenbasis des Systems (Kompetenzbereiche, Dimensionen, Kriterien, Schulen, Nationalitäten.)
- ✓ Lesender Zugriff auf die Assessmentaufgaben des Systems
- ✓ Erfassen und ändern der Selbsteinschätzung von Teilnehmern
- ✓ Zugriff auf Teilnehmer und die dazugehörigen Assessment-Aufgaben
- ✓ Reservieren der Zuständigkeit von freien Assessment-Aufgaben
- ✓ Weitergabe der Zuständigkeit für eine Aufgabe an bestimmte Benutzer
- ✓ Freigabe der Zuständigkeit für eine Aufgabe
- ✓ Erfassen von Mikrobeobachtungen (Text, Anzahl, zugeordnetes Kriterium) zu einer Teilnehmeraufgabe
- ✓ Ändern und löschen von selbst eingetragenen Mikrobeobachtungen (Text, Anzahl, zugeordnetes Kriterium)
- ✓ Erfassen, ändern und löschen der Notiz zu einer Teilnehmeraufgabe

- ✓ Lesender Zugriff auf den Tagesbericht einer Teilnehmeraufgabe
- ✓ Übertragen von Mikrobeobachtungen zwischen Teilnehmeraufgaben
- ✓ Eigene Einstellungen für die Ansicht der Teilnehmer und Assessments
- ✓ Sortieren und filtern der Teilnehmer und Assessments

8.3 B) Rechte der Berichteschreiber:

Die teilnehmerbezogenen Rechte gelten nur für die Teilnehmer, auf die der Benutzer Zugriff besitzt. Der Zugriff wird ihm dadurch erteilt, dass er Zugriff auf das Assessment erhält, in dem der Teilnehmer eingetragen ist!

- ✓ Erstellen/drucken von Gesamtberichten für Teilnehmer in Pdf-Form
- ✓ Eigene Einstellungen in den Druckoptionen
- ✓ Einsicht in alle Teilnehmeraufgaben eines Teilnehmer-Assessments
- ✓ Ändern der Zuordnung des Kriteriums zum Mikrobeobachtungstext auch für Mikrobeobachtungen, die nicht dem Benutzer gehören.
- ✓ Einsicht in die Gesamtauswertung eines Teilnehmerassessments (Alle Mikrobeobachtungen, Stärkenprofil, Ergebnisbogen, Alle Notizen, Empfehlungen, Hinweise).
- ✓ Die Kriterienzuordnung kann in der Ansicht aller Mikrobeobachtungen geändert werden.
- ✓ Bearbeiten der Empfehlung zu einem Teilnehmer
- ✓ Bearbeiten der Hinweise zu einem Teilnehmer

8.4 C) Rechte der Verwaltung:

Alle Rechte beziehen sich auf die Daten der Bildungseinrichtung des Benutzers!

- ✓ Zugriff auf alle Teilnehmer, Benutzer und Assessments
- ✓ Anlegen, ändern und löschen von Teilnehmern, Beobachten und Assessments
- ✓ Aktivieren und deaktivieren von Teilnehmern.
- ✓ Entziehen und freigeben der Zuständigkeit an Teilnehmeraufgaben
- ✓ Übertragen von Mikrobeobachtungen zwischen beliebigen Teilnehmeraufgaben

8.5 D) Rechte der Koordinatoren:

Die Benutzer mit dieser Rolle haben wenige zusätzlichen Rechte in Bezug auf die Rechte der Verwaltung.

- ✓ Anlegen, ändern und löschen von Verwaltung und Koordinatoren

Diese Rolle wird zur Unterscheidung der Verantwortlichkeit innerhalb einer Bildungseinrichtung benutzt. Änderungen in Form von erweiterten Rechten sind hier in Zukunft möglich.

8.6 E) Rechte der Hauptkoordination:

Die Rolle der Hauptkoordinatoren dient der Administration der gesamten Software, Datenbank und Einstellungen. Sie wird von Mitarbeitern der Firma MediaTec e.K. ausschließlich für die Einrichtung der vom Auftraggeber benannten Koordinatoren und für Wartungs- und Updateaufgaben genutzt.

- ✓ Einsicht in alle Daten des Systems
- ✓ Anlegen, ändern und löschen von Benutzern, Teilnehmern und Assessments für bzw. in allen Bildungseinrichtungen
- ✓ Aktivieren und Deaktivieren von jedem Benutzer des Systems
- ✓ Ändern der Datenbasis des Systems (Kompetenzbereiche, Dimensionen, Kriterien, Schulen, Nationalitäten)
- ✓ Anlegen, ändern und löschen von Assessmentaufgaben des Systems
- ✓ Anlegen, ändern und löschen von Dokumenten zu Grundinformationen
- ✓ Anlegen, ändern und löschen von Dokumenten zu Assessmentaufgaben
- ✓ Drucken des Gesamtberichts zu jedem Teilnehmer im System

9 F) Qualitätssicherung

Die Rolle der Qualitätssicherung wird noch genauer beschrieben. Sie soll auf alle Inhalte Zugriff haben, aber in den administrativen Rechten (in Bezug auf das Programm) eingeschränkt sein.

10 Rechtematrizen

10.1 Allgemeine Verwaltungsaufgaben

	A) Beob.	B) Ber.-schr.	C) Verw.	D) Koord.	E) Haupt.-koord.
Benutzer					
anlegen/	-	-	Ja (1)	Ja (1)	Ja (2)
bearbeiten/			Ja (1)	Ja (1)	Ja (2)
löschen			Ja (1)	Ja (1)	Ja (2)
aktivieren/	-	-	Ja (1)	Ja (1)	Ja (2)
deaktivieren			Ja (1)	Ja (1)	Ja (2)
Assessments					
anlegen/	-	-	Ja (1)	Ja (1)	Ja (2)
bearbeiten/			Ja (1)	Ja (1)	Ja (2)
löschen			Ja (1)	Ja (1)	Ja (2)
Teilnehmer					
anlegen/	-	-	Ja (1)	Ja (1)	Ja (2)
bearbeiten/	-	-	Ja (1)	Ja (1)	Ja (2)
löschen	-	-	Ja (1)	Ja (1)	Ja (2)

(1): Nur für die Daten der eigenen Bildungseinrichtung

(2): Für alle Daten des Systems

10.2 Systemspezifische Verwaltungsaufgaben

	A) Beob.	B) Ber.-schr.	C) Verw.	D) Koord.	E) Haupt.-koord.
Aufgaben					
anlegen/	-	-	-	-	Ja
bearbeiten/	-	-	-	-	Ja
löschen	-	-	-	-	Ja
Dokumente					
anlegen/	-	-	-	-	Ja
bearbeiten/	-	-	-	-	Ja
löschen	-	-	-	-	Ja
Bildungsein-richtungen					
anlegen/	-	-	-	-	Ja
bearbeiten/	-	-	-	-	Ja
löschen	-	-	-	-	Ja
Datenbasis					
ändern	-	-	-	-	Ja

10.3 Lesender Zugriff auf Daten

	A) Beob.	B) Ber.-schr.	C) Verw.	D) Koord.	E) Haupt.-koord.
Benutzer	-	-	Ja (1)	Ja (1)	Ja (2)
Teilnehmer	Ja (1,3)	Ja (1,3)	Ja (1)	Ja (1)	Ja (2)
Assessments	Ja (1,3)	Ja (1,3)	Ja (1)	Ja (1)	Ja (2)
Datenbasis	Ja	Ja	Ja	Ja	Ja
Aufgaben	Ja	Ja	Ja	Ja	Ja

10.4 Daten des Teilnehmer-Assessments (einzelne Aufgabe)

	A) Beob.	**B) Ber.-schr.**	**C) Verw.**	**D) Koord.**	**E) Haupt.-koord.**
Selbst-einschätzung ändern	Ja (1,3)	Ja (1,3)	Ja (1)	Ja (1)	Ja (2)
Aufgaben					
freie reservieren	Ja	Ja	Ja	Ja	Ja (2)
weitergeben/ freigeben	Ja (1,3,4)	Ja (1,3,4)	Ja (1)	Ja (1)	Ja (2)
einsehen	Ja (1,3,4)	Ja (1,3)	Ja (1)	Ja (1)	Ja (2)
Tagesbericht einsehen	Ja (1,3,4)	Ja (1,3)	Ja (1)	Ja (1)	Ja (2)
Notiz ändern	Ja (1,3,4)	Ja (1,3)	Ja (1)	Ja (1)	Ja (2)
MB eingeben	Ja (1,3,4)	Ja (1,3,4)	Ja (1,4)	Ja (1,4)	Ja (2,4)
MB (Text, Anzahl) ändern, löschen	Ja (1,3,4,5)	Ja (1,3,5)	Ja (1,5)	Ja (1,5)	Ja (2,5)
MB (Kriterium) ändern	Ja (1,3,4,5)	Ja (1,3)	Ja (1)	Ja (1)	Ja (2)

(1): Nur für die Daten der eigenen Bildungseinrichtung; (2): Für alle Daten des Systems; (3): Nur für den Benutzer explizit freigeschaltete Daten; (4): Die Teilnehmer-Aufgabe muss dem Benutzer gehören;

(5): Die Mikrobeobachtung muss dem Benutzer gehören

10.5 Daten des Teilnehmer-Assessments (alle Aufgaben)

	A) Beob.	**B) Ber.-schr.**	**C) Verw.**	**D) Koord.**	**E) Haupt.-koord.**
Aufgaben					
einsehen	-	Ja (1,3)	Ja (1)	Ja (1)	Ja (2)
alle MB einsehen	-	Ja (1,3)	Ja (1)	Ja (1)	Ja (2)
Ergebnisbogen einsehen	-	Ja (1,3)	Ja (1)	Ja (1)	Ja (2)
Stärkenprofil einsehen	-	Ja (1,3)	Ja (1)	Ja (1)	Ja (2)
alle Notizen einsehen	-	Ja (1,3)	Ja (1)	Ja (1)	Ja (2)
Empfehlung einsehen, bearbeiten	-	Ja (1,3)	Ja (1)	Ja (1)	Ja (2)
Hinweise einsehen, bearbeiten	-	Ja (1,3)	Ja (1)	Ja (1)	Ja (2)
MB (Kriterium) ändern	-	Ja (1,3)	Ja (1)	Ja (1)	Ja (2)

(1): Nur für die Daten der eigenen Bildungseinrichtung; (2): Für alle Daten des Systems; (3): Nur für dern Benutzer explizit freigeschaltete Daten

Anhang

Sicherheitskonzept NMMN