Universität Zürich[UZH]

Institut für Volkswirtschaftslehre / Digital Society Initiative

Z-Pool-Tool

Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept)

Andreas Saurer, Markus Christen

Version 2.3, August 2025

Inhaltsverzeichnis

EINLEITUNG **4**

1 Ziel des ISDS **4**

2 Rechtsgrundlagen **4**

3 Geltungsbereich / Abgrenzungen **5**

4 Ansprechpartner und Verantwortlichkeiten **5**

SICHERHEITSRELEVANTE SYSTEMBESCHREIBUNG **6**

5 Gesamtsystem / Applikation **6**

RISIKOANALYSE **8**

SCHUTZMASSNAHMEN **9**

6 Rollen und deren Autorisierung **9**

6.1 Betreiber/Nutzergruppen und zugehörende Rollen 9

6.2 Autorisierung von Rollen 10

7 Authentisierung **11**

7.1 Authentisierungsverfahren 11

8 Logging und Monitoring **11**

8.1 Logging 11

8.2 Monitoring 12

SICHERSTELLUNG DES GESCHÄFTSBETRIEBS INKL. NOTFALLKONZEPT **12**

9 Wartung / Change Management **12**

9.1 Wartung und Anpassung der Z-Pool-Tool Technologie 12

9.2 Wartung und Anpassung der einzelnen Pools 12

10 Notfall-Konzept (Business Continuity Management BCM) **13**

10.1 Notfall-Konzept für die Z-Pool-Tool Technologie 13

10.2 Notfall-Konzept für die einzelnen Pools 13

ANHANG **15**

11 Einstufung Risiko **15**

11.1 Risikomatrix 15

11.1.1 Eintrittswahrscheinlichkeit (E) 15

11.1.2 Schadensausmass (S) 16

11.1.3 Berechnung 16

EINLEITUNG

1 Ziel des ISDS

Das Informationssicherheits- und Datenschutz-Konzept (ISDS) beschreibt die sicherheitsrelevanten Aspekte des Z-Pool-Tool und des späteren Betriebs der IT-Infrastruktur. Die Schwerpunkte der Betrachtung liegen auf:

- den Rechtsgrundlagen
- dem Schutzbedarf und den Sicherheitsvorgaben
- der sicherheitsrelevanten Projektbeschreibung;
- der Analyse der Risiken;
- den Rollen und den Berechtigungen der verschiedenen Nutzergruppen
- und dem Handlungsbedarf (zu ergreifenden Massnahmen).

Der Begriff «Z-Pool-Tool» bezeichnet dabei zweierlei: Zum einen die Technologie an sich (Software), die Gegenstand des vorliegenden ISDS-Konzepts ist. Zum anderen den Namen einer (designierten) UZH-Technologieplattform, welche für die Wartung und den Betrieb dieser Software zuständig ist.

2 Rechtsgrundlagen

Das «Z-Pool-Tool» stellt eine technische Grundlage in Form einer (Software) für die studienbedarfsspezifische Bildung und Verwaltung von Probanden-Pools für alle in der Humanforschung tätigen Mitarbeitenden an DIZH Hochschulen (PHZH, UZH, ZHAW, ZHdK) sowie der ETH Zürich bereit und ermöglicht die Rekrutierung von Probanden sowie deren Buchung für Studien. Die UZH ist Urheberin des Z-Pool-Tools und damit alleinige Inhaberin des geistigen Eigentums an der Software «Z-Pool-Tool».

Das Z-Pool-Tool selbst stellt keine Datenbank dar, sondern eine Software, mit welcher sich Datenbanken aufbauen und verwalten lassen. Solche Datenbanken bestehen aus Kontaktdaten und weiteren Deskriptoren (wie z.B. Alter und Geschlecht) von Personen, die Ihre Zustimmung zur Teilnahme an Studien unterschiedlicher Art gegeben haben. Das Z-Pool-Tool ermöglicht es, innerhalb solcher Datenbanken die für bestimmte Studien jeweils geeigneten Personen anzufragen, ob sie konkret an der jeweiligen Studie teilnehmen wollen oder nicht – eine Teilnahme an einer einzelnen Studie erfolgt immer erst nach Zustimmung der betreffenden Person. Mit dem Z-Pool-Tool werden zudem keine studienbezogenen Daten gesammelt.

Die durch das Z-Pool-Tool verwalteten Datenbanken selbst bestehen bereits (teilweise seit mehr als 10 Jahren) an verschiedenen Instituten der UZH und anderen Hochschulen des Kantons Zürich und werden aktuell mit veralteten Systemen verwaltet. Das Z-Pool-Tool ersetzt diese alten Systeme mit einer neuen Software, welche den heutigen Anforderungen an Datensicherheit besser entspricht.

Eingebettet ist die Z-Pool-Tool-Technologie in eine institutionelle Struktur – konkret eine Technologieplattform der UZH; ebenfalls «Z-Pool-Tool» genannt. Diese institutionelle Struktur stellt die technische Wartung der Software sicher und sorgt für die Schulung der Nutzer der Technologie – insbesondere auch hinsichtlich der Wahrung des Datenschutzes. Formale Aspekte der Technologieplattform sind in deren Geschäftsordnung und den Allgemeinen Geschäftsbedingungen festgehalten.

3 Geltungsbereich / Abgrenzungen

Das Z-Pool-Tool wird auf virtuellen Server der Zentralen Informatik (ZI) der Universität Zürich betrieben (*managed server*). Die Datenbank-Server werden ebenfalls von der ZI betrieben und unterliegen damit den generellen Sicherheitsmassnahmen der UZH Informatik. Diese Systeme werden deshalb in diesem Konzept nicht weiter betrachtet.

4 Ansprechpartner und Verantwortlichkeiten

Mit Blick auf die Technologieplattform Z-Pool-Tool als Ganzes bestehen folgende Ansprechpartner und Verantwortlichkeiten (siehe auch Abschnitt 6 für die genauen Bezeichnungen der einzelnen Nutzergruppen des Z-Pool-Tools). Für den institutionellen Aufbau der Technologieplattform wird zudem auf die Geschäftsordnung verwiesen.

Rolle	Kontakt	Abteilung	Aufgaben
Projektleitung und designierter Betreiber	markus.christen@dsi.uzh.ch	DSI-Geschäftsstelle (Geschäftsleiter)	Primäre Anlaufstelle für Anfragen von Primärnutzern.
Anwendungsverantwortlicher	it@econ.uzh.ch	IVW, IT Team	Wartung und Weiterentwicklung der Software
Systembetreiber	lnxhosting@zi.uzh.ch	ZI, Linux & Identity Services	Wartung der virtuellen Server
IT Sicherheitsbeauftragter	security@zi.uzh.ch	ZI, IT Sicherheit	CSIR
Dateninhaber	Jeder Primärnutzer selbst. Siehe dazu auch Abschnitt 6		Betreuung Pools und Kontaktdaten

Hinweis: Aktuell ist das Z-Pool-Tool immer noch in der Aufbauphase – die Etablierung als UZH-Technologieplattform mitsamt den oben genannten Verantwortlichkeiten wird erst nach Abschluss der kantonalen Datenschutzprüfung erfolgen.

Es ist weiter festzuhalten, dass das Z-Pool-Tool als Technologieplattform selbst kein Dateninhaber ist (dies sind die einzelnen Primärnutzer bzw. Pool-Inhaber) mit einer Ausnahme: Das Z-Pool-Tool wird den bisher vom UZH-Rektoratsdienst gemanagten «Rektorats-E-Mail-Versand» für den Versand von Studienanfragen übernehmen (UZH-Pool). Damit soll eine klare Trennung zwischen dem Versand von E-Mails für Studienanfragen und solchen für andere UZH-betreffenden Informationen geschaffen werden. Damit wird insbesondere auch sichergestellt, dass von sämtlichen Personen, die für die Teilnahme an Studien angefragt werden können, eine entsprechende Einwilligung besteht, die auch jederzeit widerrufen werden kann. Dieser Punkt war in der alten technischen Lösung bislang nicht gewährleistet worden.

Die Z-Pool-Tool-Technologie wird es erlauben, dass diese Personen ihre Bereitschaft zur Teilnahme an Studien jederzeit einfach widerrufen können, was zur Löschung aller persönlichen Daten im Pool führen wird.

Die konkreten Verantwortlichkeiten der Dateninhaber (Primärnutzer) sind in den Allgemeinen Geschäftsbedingungen festgelegt. Durch Schulung und Controlling/Reporting wird sichergestellt, dass diese die Vorschriften bezüglich Datenschutz und Datensicherheit einhalten.

SICHERHEITSRELEVANTE SYSTEMBESCHREIBUNG

5 Gesamtsystem / Applikation

Die Software «Z-Pool-Tool» ist auf zwei Virtuellen Server (managed server, zieconweb01 und 02) der UZH ZI installiert. Diese Server werden mit Red Hat Enterprise Linux 8 betrieben und von der ZI gewartet. Zugriff auf die Server ist nur durch wenige Personen (ZI, Econ IT) über einen SSH Proxy aus dem UZH Netzwerk möglich. Beide Server sind analog aufgebaut, verfügen zwecks Ausfallsicherheit über separate Update Zyklen.

Die Server stehen im Datacenter Irchel der ZI. Über Zugang und Absicherung des Datacenter mach die ZI aus Sicherheitsgründen keine Angaben. Eine Firewall ist vorhanden worauf nur Port 80, sowie 443 gegen aussen für die Server des Z-Pool-Tools freigegeben sind. Durch einen Loadbalancer werden Anfragen auf die beiden Server zieconweb01 und 02 verteilt. Ausgehende Verbindungen vom Server in das Internet werden.

Auf den Servern läuft ein Nginx Webserver, welcher die Anfragen entgegennimmt und über proxying an den Z-Pool-Tool Prozess weitergibt. Der Z-Pool-Tool Prozess hört auf zwei verschiedenen Ports, über einen wird die *Root-Komponente* und über den anderen alle *Tenant-Komponente* angesprochen.

Über die *Root-Komponente* werden Pools (*Tenant*) erfasst und verwaltet. Hierbei werden Grundeinstellungen gespeichert, welche zur Verbindung zum Tenant notwendig sind (URL, Datenbank Zugangsdaten). Zugangsdaten werden verschlüsselt abgelegt und können nur eingegeben werden, es ist nicht möglich über die Benutzeroberfläche die Zugangsdaten zu lesen. Eine Änderung dieser, erfordert die Eingabe des kompletten «*MariaDB Connection Strings*». Zugriff auf die *Root-Komponente* ist nur aus dem UZH NAC IP Admin Bereich, sowie dem IP Bereich der Schönberggasse (Standort des Econ IT Team) und durch Eingabe eines Logins möglich.

Die *Tenant-Komponente* ist für die Anzeige eines Pools verantwortlich. Über den Request Header wird die gewünschte URL ausgelesen, die entsprechenden Datenbank Zugangsdaten in der Root Datenbank gesucht und eine Verbindung zur Tenant Datenbank aufgebaut. In der Tenant Datenbank sind die Daten des Pools (Probanden mit Personenbezogenen Daten, Studien, Studienteilnahmen) gespeichert.

Das Z-Pool-Tool verwendet zum Versand von E-Mails externe SMTP Server. Die SMTP-Account Informationen dazu werden in der Tenant Datenbank abgelegt. Hierbei wird das Passwort verschlüsselt und kann – wie im Root – über die Benutzeroberfläche nur neu gesetzt und nicht ausgelesen werden. Die Verbindung zum SMTP Server erfolgt mit den bei der Eingabe gewählten Verschlüsselungsmechanismen. Wo ein solcher SMTP Server steht ist jedem Primärnutzer überlassen.

Ebenfalls lässt sich ein «API Key» für den Versand von SMS über einen Gateway speichern. Daten werden mittels HTTPS an den Gateway übermittelt. Auch hier ist dem Primärnutzer überlassen welcher Dienst und somit Ort benutzt wird.

In der Abbildung 1 wird ein UZH Pool (Tenant 1) mit einer Datenbank im ZI Datacenter Irchel und einem zweiten Pool (Tenant 2) mit Datenspeicherort ZHAW aufgezeigt. Im Falle der UZH wird der

SMTP Server von Microsoft betrieben, wo genau sich dieser befindet ist durch die Natur verteilter Systeme nicht eindeutig zu bezeichnen.

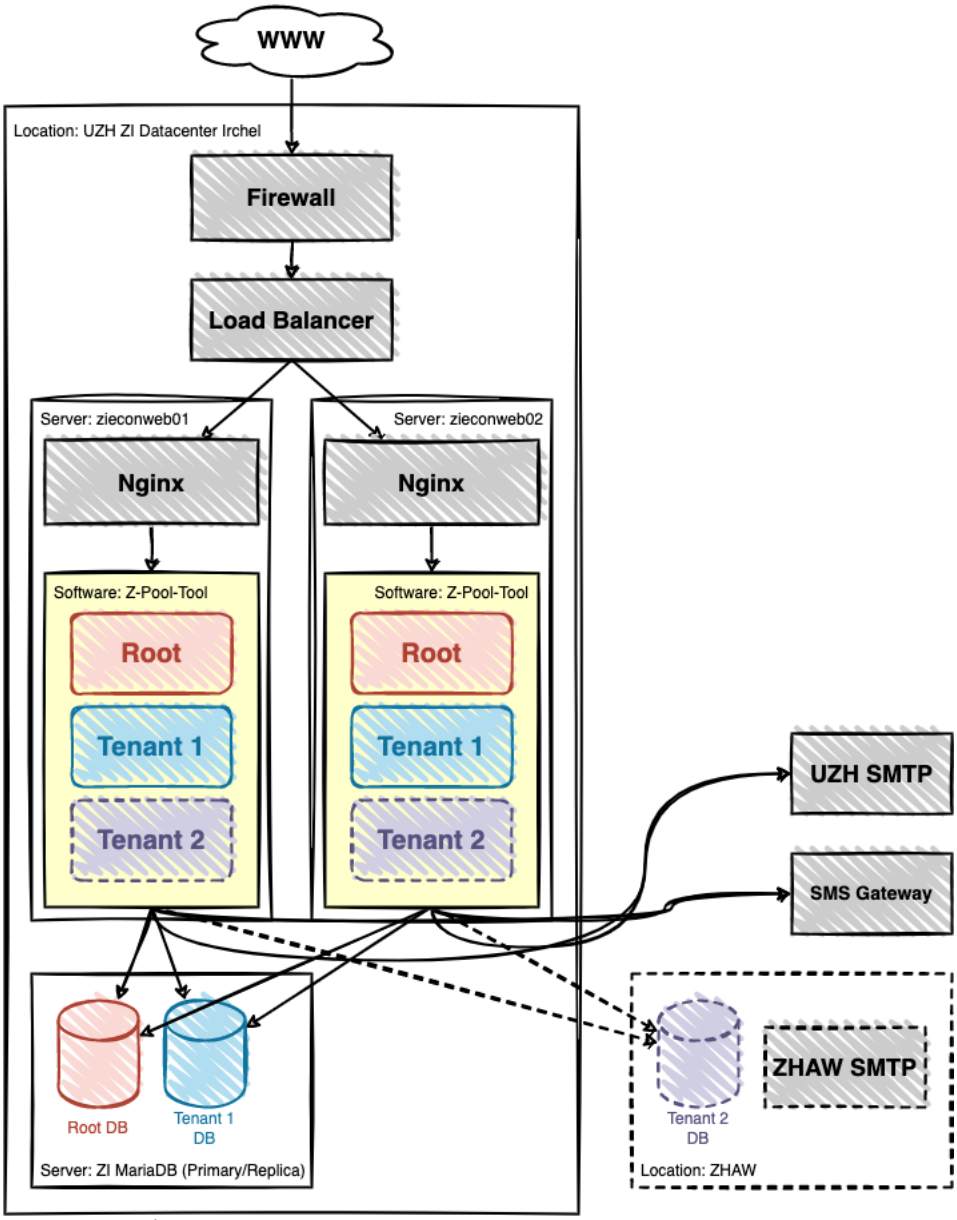

Abbildung 1 Architekturdiagramm

RISIKOANALYSE

Von der IT-Sicherheitsstelle der UZH wurde im April 2023 ein Penetration Test durchgeführt, Details sind dem entsprechenden Dokument zu entnehmen. Nachfolgend werden die grössten Risiken beschrieben und eingestuft.

Die untenstehenden Risiken wurden dem Konzept für die Datenschutz -Folgeabklärung (DSFA) entnommen. Hierbei werden Risiko 1 und 3 der DSFA zusammen betrachtet, da die Formulierung allein für eine Bewertung Interpretationsspielraum lässt.

#	A) Inhärentes Risiko	B) Bewertung	C) Massnahme	D) Restrisiko
1, 3	**Ansammlung von Daten** (d.h. Namen, E-Mail und eventuelle andere Daten von mehr als 10'000 Personen) **Hohe Anzahl betroffener Personen** im Falle eines Data-Breaches bei einem grossen Pool	5 * 5 = 25	• Es werden nur notwendige Daten gespeichert • Datenzugriff innerhalb eines Pools basiert auf definierten Rollen (siehe dazu Abschnitt 6), Zugriff nur wo notwendig • Primärnutzer akzeptieren AGB der technologieplattform mit den dort festgehaltenen Pflichten. • Daten-Attribute werden kategorisiert und nach Rollen eingeschränkt • Der Zugriff auf Listenansichten von Kontaktdaten ist gemäss Rollenkonzept eingeschränkt, nur definierte Rollen können solche Listen sehen und Probanden-Daten editieren. Die Zuweisung der Rolle wird individuell für jeden Pool vom jeweiligen Primärnutzer vorgenommen. • Kontaktdaten von Proband:innen werden nur mit erweiterten Rechten und in notwendigem Kontext angezeigt	3 * 2 = 6
2	Trennung zwischen Personen- und Studiendaten – **Restrisiko Datenverknüpfungen**	3 * 3 = 9	• Datenzugriff basiert auf Rollen, Zugriff nur wo notwendig • Daten-Attribute werden kategorisiert und nach Rollen eingeschränkt • Kontaktdaten von Proband:innen werden nur mit erweiterten Rechten und in notwendigem Kontext angezeigt • Studiendaten werden nicht im System gespeichert	2 * 3 = 6

SCHUTZMASSNAHMEN

6 Rollen und deren Autorisierung

6.1 Betreiber/Nutzergruppen und zugehörende Rollen

Grundsätzlich werden vier Arten von Betreiber-/Nutzergruppen des Z-Pool-Tools unterschieden mit jeweils definierten Rollen:

Gruppe 1 - Betreiber: Dies ist die für den Betrieb der Technologieplattform Z-Pool-Tool verantwortliche Organisationseinheit der UZH. Sie vergibt Nutzungsrechte an Primärnutzer (siehe Abschnitt 6.2.). Der Z-Pool-Tool-Betreiber legt fest, wer einen Pool mit der Z-Pool-Tool-Technologie betreiben darf und stellt sicher, dass die relevanten datenschutzrechtlichen Bestimmungen eingehalten bzw. den Primärnutzern zur Kenntnis gebracht werden. Die entsprechenden Bestimmungen sind in den AGBs geregelt. Folgende Rollen sind der Gruppe 1 (Betreiber) zugeordnet:

- ***Rolle 1.1 – Verwaltung:*** Die formell verantwortliche Einheit der UZH (geplant: Digital Society Initiative; aktuell hat die DSI die Projektleitung). Personell wird die Verantwortung durch den Geschäftsführer der DSI wahrgenommen. Eine zweite Person der DSI-Geschäftsstelle figuriert als Ansprechperson für die Primärnutzer.
- ***Rolle 1.2 – Technik*** *(root):* Die für den technischen Betrieb und die Weiterentwicklung des Z-Pool-Tools verantwortliche Einheit der UZH (Department of Economics, ECON). Personell besteht dies durch den Leiter der Informatik der ECON und seinem Team. Das Team hat Zugriff auf die zugrundeliegende Infrastruktur.

Gruppe 2 – Primärnutzer: Dieser Begriff bezeichnet eine Organisationseinheit, die für die Erstellung und Pflege eines Pools verantwortlich ist und damit Nutzungsberechtigter der Z-Pool-Tool-Technologie ist. Ein Primärnutzer ist in der Regel durch eine verantwortliche Person einer Organisationseinheit repräsentiert (z.B. Institut oder Forschungsgruppe) einer DIZH Hochschule oder der ETH Zürich, Ausnahmen sind möglich. Einem Primärnutzer sind mehrere Funktionen und damit auch Rolle zugeordnet, die Aufgaben rund um die Nutzung eines Pools wahrnehmen. Je nach Grösse des Pools können diese Rollen durch eine oder mehrere Personen wahrgenommen werden:

- ***Rolle 2.1. – Pool-Besitzer****:* Der juristisch gesehen formelle Besitzer eines Pools und damit auch Dateninhaber (z.B. ein Institut, vertreten durch den Institutsleiter). Unter anderen ist es seine Verantwortung, dass die datenschutzrechtlichen Verpflichtungen, die mit dem Betrieb eines Pools verbunden sind, eingehalten werden.
- ***Rolle 2.2. – Pool-Betreiber*** *(operator):* Die technisch verantwortliche Person für den Unterhalt eines Pools. Er nutzt das System hauptsächlich über die Desk-Top-Website und hat Zugriff auf die Datenbank des jeweiligen Pools und eventuell auch auf den Mailserver, übr den die Einladungs-E-Mails laufen. Er hat keinen Zugriff auf den Server, auf dem das Z-Pool-Tool läuft.. Er ist der technischen Partner des Rekrutierers.
- ***Rolle 2.3. – Rekrutierer*** *(recruiter):* Person, die für die Rekrutierung von Probanden für den Pool selbst wie auch für die Rekrutierung von Probanden aus dem Pool für einzelne Studien verantwortlich ist. Der Rekrutierer nutzt das System hauptsächlich über die Desktop-Website. Er hat keinen Zugang auf die Datenbank des jeweiligen Pools als Ganzes; er kann nur Abfragen in der Datenbank machen.
- ***Rolle 2.4. – Standortleiter*** *(location manager):* Die Person, welche gewisse Aufgaben (z.B. Betreuung der Location) für die Durchführung einer einzelnen Studie vor Ort wahrnimmt, sofern

es sich bei der Studie um ein physisch durchgeführtes Laborexperiment handelt (im Fall einer Online-Befragung wird diese Rolle nicht wahrgenommen). Der Standortleiter hat ausschliesslich Lesezugriff auf die Liste der Probanden, die für das jeweilige Experiment am jeweiligen Standort aufgrund ihrer Zustimmung zur Teilnahme am Experiment anwesend sein sollten.

Gruppe 3 – Sekundärnutzer: Dieser Begriff bezeichnet jene Person, die eine einzelne Studie durchführt und dafür die Rekrutierung von Probanden eines Pools, der durch das Z-Pool-Tool verwaltet wird, in Anspruch nimmt. Ein Sekundärnutzer ist in der Regel ein:e Forscher:in einer DIZH-Hochschule oder der ETH Zürich oder ein:e Mitarbeiter:in aus dem Rekrutierungsteam, Ausnahmen sind möglich. Je nach Umfang der einzelnen Studie gehören folgende Rollen zu dieser Gruppe:

- ***Rolle 3.1. – Experimentator*** *(experimenter):* Die für eine Studie, welche mit Hilfe der Probanden eines bestimmten Pools durchgeführt wird, verantwortliche Person. Sie definiert die Kriterien, anhand derer Anfragen an Probanden des Pools für die Teilnahme an der Studie erfolgen. Der Experimentator benutzt das System zu informativen zwecken (Datum der Sessions, Belegung der Sessions). Diese Person führt in gewissen Fällen (z.B. Einzel-Sessions) die Studie vor Ort durch, in diesem Fall wir die Rolle mit zusätzlichen Rechten erweitert, damit die Teilnehmerliste eingesehen werden kann.
- ***Rolle 3.2 – Assistenz*** *(assistant):* Personen, welche je nach Grösse der Studie definierte Aufgaben bei der Interaktion mit den Probanden wahrnimmt, z.B. Kontrolle der Anwesenheitsliste, die Bezahlung der Probanden vor Ort. In gewissen Fällen (Einzel-Sessions) wird diese Aufgabe vom Experimentator selbst wahrgenommen.

Gruppe 4 – Probanden (*contact*)**:** Dieser Begriff bezeichnet eine Person, die aufgrund einer informierten Zustimmung Teil eines Pools ist und von einem Sekundärnutzer für die Teilnahme an einem Experiment angesprochen werden kann; für diese Teilnahme ist wiederum eine informierte Zustimmung nötig. Probanden sind Personen mit Wohnsitz in der Schweiz aufgrund einer Selbstdeklaration. Sie können einen Pool jederzeit ohne Angabe von Gründen selbständig verlassen oder ihren Account pausieren.

6.2 Autorisierung von Rollen

Wir beschreiben nachfolgend die Autorisierung der Rollen für die verschiedenen Nutzergruppen.

Rolle	**Technische Zugriffsrechte auf Z-Pool-Tool**	**Autorisierung durch**	**Kriterien**
Betreiber Technologieplattform	Keine (technischer Zugriff erfolgt durch «Technik»)	Konstituiert sich selbst	Siehe Geschäftsordnung
Technik Technologieplattform	Root (nur auf die Root Instanz)	Betreiber Technologieplattform	Siehe Geschäftsordnung
Pool-Besitzer	Keine	Betreiber Technologieplattform	Siehe AGBs der Technologieplattform
Pool-Betreiber	Alle möglichen Rechte auf System, Probanden, Experimente	Pool-Besitzer	Siehe AGBs der Technologieplattform
Rekrutierer	System-Einstellungen verwalten (ausser E-Mailserver), Probanden verwalten, Experimente verwalten	Pool-Besitzer	Siehe AGBs der Technologieplattform

Standortleiter	Spezifischen Standort verwalten, Sessions und Teilnahmen am Standort sehen	Pool-Besitzer	Siehe AGBs der Technologieplattform
Experimentator	Spezifisches Experiment sehen. In Ausnahmefällen vom spezifischen Experiment: Session-Teilnehmende und deren Kontaktdaten sehen, Session Anwesenheitsliste führen	Pool-Besitzer	Gemäss Kriterien des Pool-Besitzers
Assistenz	Session-Teilnehmende und deren Kontaktdaten sehen, Session Anwesenheitsliste führen	Experimentator	Gemäss Kriterien Experimentator
Proband:in	Eigenes Profil via Login	Formell: Pool-Besitzer Materiell: Rekrutierer	Gemäss Kriterien des Pool-Besitzers

7 Authentisierung

Der Anwenderkreis der Software entspricht der unter Kapitel 6 «Rollen und deren Autorisierung» definierten Rollen. Das verwendete Authentisierungsverfahren ist für alle Rollen dasselbe und wird im folgenden Kapitel aufgezeigt.

7.1 Authentisierungsverfahren

Ein Login für die Technik *(root)* oder zu einem Pool *(tenant)* ist unabhängig voneinander, erfolgt aber über denselben Mechanismus (Password-Hash). Beide Logins werden bis August 2025 auf Zwei-Faktor Authentifizierung erweitert.

Für jede:n neue:n oder importierte:n Benutzer:in wird ein Initialpasswort vergeben, welches von der/dem jeweiligen Benutzer:in selbständig geändert und zurückgesetzt werden kann.

Die Login-Informationen sind verschlüsselt in der jeweiligen Datenbank abgelegt, sowie auch die Daten der Login-Formulare nur verschlüsselt übertragen werden. Danach wird ein Session Cookie gespeichert. Vergleiche auch Penetration Test Report.

Zusätzlich zum Login, ist der Zugriff auf die *Root-Komponente* nur aus dem UZH NAC IP Admin Bereich möglich.

8 Logging und Monitoring

8.1 Logging

Die folgende Tabelle zeigt die durch die Applikation und den Server erstellte Logs. Solche Logs können Personenspezifische Daten (z.B. IP-Adresse) beinhalten. Diese Logs dienen der Sicherstellung des Betriebes und der Fehleridentifizierung.

Typ	**Zweck**	**Aufbewahrung**	**Zeitraum**	**Zugriff**
Serverlogs	Fehlerfindung, Zugriffskontrolle, Security	Server	11 Wochen	Econ IT Team

Activity Log	Übersicht über Aktivitäten im Tenant	Tenant Datenbank	Keine definierte Löschung (manuell)	Tenant Operator, Tenant Recruiter

8.2 Monitoring

Es findet ein allgemeines Monitoring des Status der Dienste (Prozesse auf dem Server) und der Erreichbarkeit der Webseite mittels Software «Nagios» statt. Nagios wird von der ZI betrieben, alarmiert werden Mitarbeitende der ZI, sowie des Econ IT Teams.

SICHERSTELLUNG DES GESCHÄFTSBETRIEBS INKL. NOTFALLKONZEPT

9 Wartung / Change Management

9.1 Wartung und Anpassung der Z-Pool-Tool Technologie

Die Wartung der Z-Pool-Tool Technologie (also der Software) wird von der Technologieplattform wahrgenommen – konkret vom technischen Team (Anwendungsverantwortlichen). Dies umfasst Korrektur von Bugs, die im Betrieb auftauchen und von den Primärnutzern der Technologieplattform gemeldet werden, sowie Patching der Software in regelmässigen Abständen (min. halbjährlich). Das Betriebssystem und die damit verbundene Software wird von der ZI, gemäss deren Serviceagreement, in regelmässigen Abständen gewartet.

Anpassungen an der Technologie (z.B. Erfassen neuer technischer Features) werden ebenfalls vom technischen Team wahrgenommen. Der Prozess zur Etablierung und Genehmigung neuer Features ist in der Geschäftsordnung der Technologieplattform beschrieben.

9.2 Wartung und Anpassung der einzelnen Pools

Die Wartung der einzelnen Pools (also konkret die Prozesse zur Ergebung und Verwaltung der Einwilligungen der Probanden im Pool, die Sicherstellung der Löschung von Daten aus dem Pool und weitere datenschutzrechtliche Aktivitäten) liegt in der Verantwortung der einzelnen Pool-Besitzer. Diese Verantwortung wird in einer schriftlichen Vereinbarung zwischen der Technologieplattform und dem Primärnutzer festgehalten; die Modalitäten (Rechte und Pflichten der Vertragsparteien) sind in den allgemeinen Geschäftsbedingungen festgehalten.

Anpassungen an den Pool selbst (z.B. die Definition neuer Charakteristika zur Stratifizierung des Pools gemäss den spezifischen Bedürfnissen des Pools) können ebenfalls vom Primärnutzer unter Einhaltung der in den allgemeinen Geschäftsbedingungen festgehaltenen Rahmenbedingungen vorgenommen werden.

Die einzelnen Pool-Betreiber sind verpflichtet, in einem jährlichen Report Anpassungen am Pool, Nutzung des Pools, Sicherheitsvorfälle etc. zu melden. Die entsprechenden Details sind ebenfalls in den allgemeinen Geschäftsbedingungen festgehalten.

10 Notfall-Konzept (Business Continuity Management BCM)

Es werden nachfolgend drei Arten von relevanten Notfällen unterschieden gemäss der CIA-Triade für Cybersicherheit:

1) Bruch der *Confidentiality*: Es kommt zu einem grossen Abfluss von Personendaten aus einem oder mehreren Pools aufgrund eines unberechtigten Zugriffs.
2) Bruch der *Integrity*: Die Korrektheit der Daten in einem oder mehrerer Pools ist nicht mehr gewährleistet.
3) Bruch der *Availability*: Die Software kann nicht genutzt werden und entsprechend können keine Experimente mit dem Z-Pool-Tool mehr organisiert werden.

10.1 Notfall-Konzept für die Z-Pool-Tool Technologie

Massgebend für die Technologieplattform als Ganzes sind insbesondere der Bruch der *Confidentiality* (für alle Pools) und der Bruch der *Availability* (in gewissem Mass auch der Bruch der *Integrity*, weil die Technologieplattform auch den UZH-Pool managen soll).

In allen Fällen der CIA-Triage soll ein mehrstufiges Verfahren eingesetzt werden, abhängig von der Grösse und Tragweite des Bruches:

- Stufe 1: Sofortige Einschränkung des Zugriffes auf die Pools (Ausschluss von Netzwerk-Anfragen aus dem IP-Bereich / Landes des Angriffes). Im Falle eines Bruches der *Confidentiality* werden die Betroffenen und die Leitung der Technologieplattform informiert.
- Stufe 2: Weitere sofortige Einschränkung des Zugriffes auf die Software (Zugriffe nur aus dem UZH-Netzwerk möglich). Absprachen der Leitung der Technologieplattform, des technischen Teams und allenfalls der ZI.
- Stufe 3: Komplette temporäre Deaktivierung der Software.

Die Einstufung wird durch die Leitung der Technologieplattform auf Empfehlung des technischen Teams getroffen.

Alle Stufen eines Bruches ziehen eine Überprüfung der Logfiles, sowie der Technologie zu Folge. Die Leitung der Technologieplattform (in Absprache mit dem technischen Team und/oder der ZI) entscheidet über eine Durchführung eines Penetration Tests, bevor die Software wieder für alle zugänglich gemacht wird.

10.2 Notfall-Konzept für die einzelnen Pools

Die Ausarbeitung eines Notfall-Konzeptes für die einzelnen Pools unterliegt grundsätzlich den einzelnen Primärnutzern (Pool-Besitzern), was in den AGBs festgehalten und auch Teil der Vereinbarung zwischen der Technologieplattform und dem Primärnutzer ist. Diese Notfall-Konzepte orientieren sich an folgenden Prinzipien:

- Bruch der *Confidentiality*: Kommt es zu einem unautorisierten Datenabfluss aus einem Pool, ist sofort die Technologieplattform zu informieren, so dass gemeinsam (eventuell auch unter Einbezug der Zentralen Informatik der UZH) Gegenmassnahmen getroffen werden können. Art und Ausmass dieser Gegenmassnahmen wird unter anderem von der Grösse des Pools und der Art der Daten (sind besondere Personendaten betroffen?) abhängen.
- Bruch der *Integrity*: Die Wahrung der Integrität liegt in direktem Interesse der Primärnutzer (sonst würden z.B. Personen für Experimente eingeladen, die es gar nicht mehr gibt). Die AGBs

halten fest, welche konkreten technischen Massnahmen jeder Primärnutzer umsetzen muss, um die Integrität der Daten sicherzustellen.

- Bruch der *Availability*: Auch dies liegt im direkten Interesse der Primärnutzer. Allerdings dürfte ein Bruch der *Availability* in der Regel mit generellen Software-Problemen zusammenhängen, was dann in die Verantwortung der Technologieplattform fällt.

ANHANG

11 Einstufung Risiko

11.1 Risikomatrix

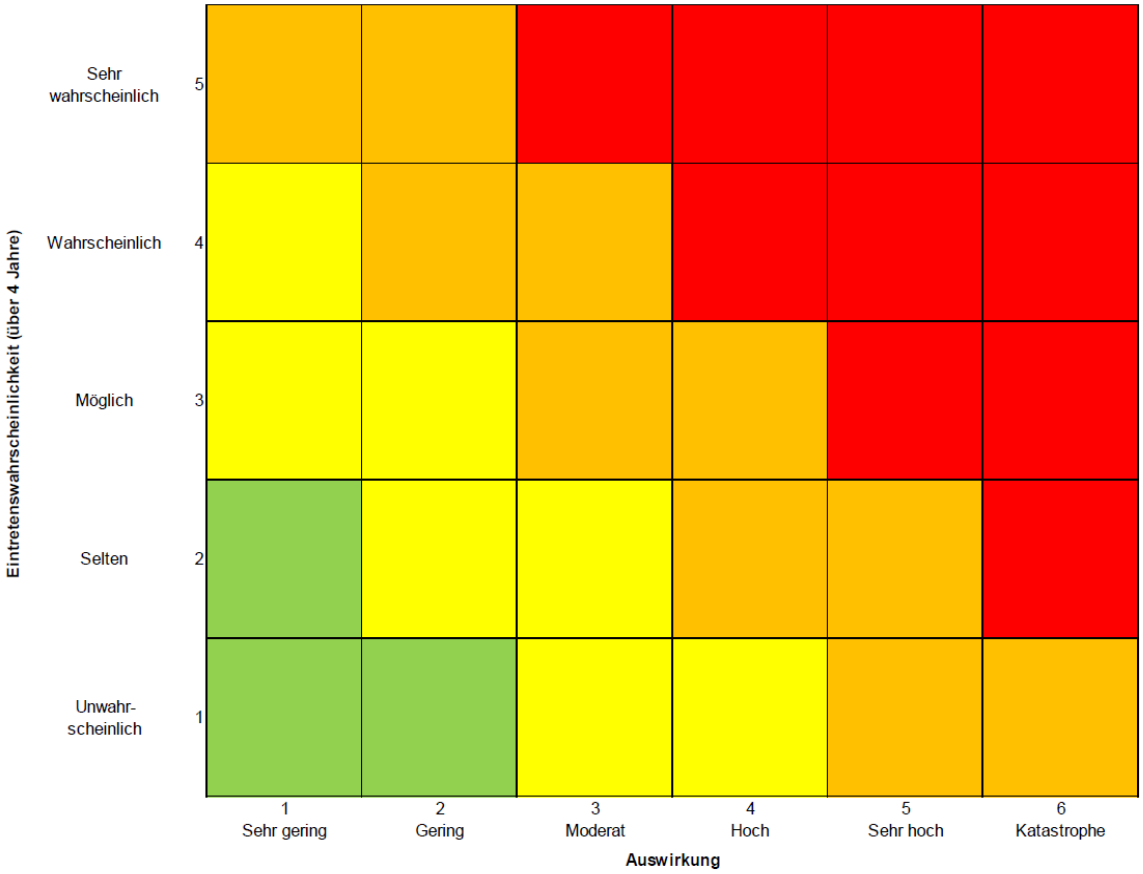

Abbildung 5: Risikomatrix

11.1.1 Eintrittswahrscheinlichkeit (E)

Skala	Eintrittswahrscheinlichkeit	Mögliche Eintrittsrate
5	sehr wahrscheinlich	> 90%
4	wahrscheinlich	51% - 90%
3	möglich	31% - 50%
2	selten	11% - 30%
1	unwahrscheinlich	≤10%

11.1.2 Schadensausmass (S)

Auswirkungen	Sehr gering	Gering	Moderat	Hoch	Sehr hoch	Kata-strophe
In Fr.	1	2	3	4	5	6
Finanzielle Auswirkungen	≤10'000	> 10'000-100'000	> 100'000-1 Mio.	> 1 Mio. - 10 Mio.	> 10 Mio. - 50 Mio.	> 50 Mio.

Skala	Kate-gorie	Beschreibung	
		Auswirkung auf Leistungsfähigkeit	Auswirkung auf Zielsetzungen des Leistungsauftrags (inkl. Einhaltung Termine und Budget)
1	Sehr gering	Bleibt erhalten	Keinen Einfluss
2	Gering	Geringfügig beeinträchtigt	Leichte Anpassungen notwendig, um Zielsetzungen zu erreichen
3	Moderat	Leicht reduziert	Moderate Anpassungen notwendig, um Zielsetzungen zu erreichen
4	Hoch	Spürbar	Anpassungen notwendig, um Zielsetzungen zu erreichen
5	Sehr hoch	Beträchtlich reduziert	Grössere Anpassungen notwendig, um Zielsetzungen zu erreichen
6	Katastro phe	Langfristig verloren	Erhebliche Anpassungen notwendig, um Zielsetzungen zu erreichen

Das Schadensausmass wird nicht nur monetär beurteilt, sondern eingerechnet sind auch Reputations-schaden und allfällige Gerichtskosten.

11.1.3 Berechnung

Übertragen in die Risikoanalyse des ISDS-Konzeptes wird «nur» der Wert Schadensaus-mass * Eintre-tenswahrscheinlichkeit gemäss Matrix. Beispiele: E=3 * S=2 = 6 (Gelb) oder E=1 * S=6 = 6 (Orange).