TYPO3: Sicherheitsorientierte Neukonzeption des Berechtigungs- und Qualifizierungsmodells

1. Zielsetzung

Die Webseiten der Universität Kassel stellen ein zentrales Aushängeschild der Hochschule dar. Um ihre Professionalität, Auffindbarkeit, Barrierefreiheit sowie Rechtskonformität – insbesondere in Hinblick auf Urheberrecht, Datenschutz und den AI Act – zu gewährleisten, dürfen Inhalte ausschließlich von geschulten und zertifizierten Redakteur:innen veröffentlicht werden.

Neben der inhaltlichen Qualitätssicherung hat die Sicherheit des Webauftritts eine besondere Bedeutung. Ungeschulte oder unzureichend qualifizierte Personen erhöhen das Risiko von Fehlbedienungen, sicherheitsrelevanten Eingriffen, unbeabsichtigten Änderungen oder Löschungen mit unwiderruflichen Datenverlusten und belasten gleichzeitig über die Maßen die vorhandenen Supportkapazitäten.

Ein sicherheitsorientiertes Nutzungsmodell setzt daher voraus, dass Zugänge nur an Personen vergeben werden, die die notwendigen Kenntnisse nachweislich erworben haben. Das aktuelle Nutzungsmodell soll in eine sicherheitsorientierte Anwendungslogik transformiert werden. Dazu gehört auch eine Modifizierung der Accountvergabe, die aktuell dezentral und nach einem „Schnellballsystem“ vergeben werden. Dieses stetig unkontrollierte Anwachsen des Accountbestandes bietet eine erhebliche digitale Angriffsfläche: Moderne, KI-gestützte Angreifer können Zugänge automatisiert identifizieren und kompromittieren. Weniger Accounts bedeuten weniger Passwörter, die durch Social Engineering, Phishing oder Brute-Force-Angriffe erraten oder gestohlen werden können.

2. Ausgangssituation

Viele RedakteurInnen arbeiten schon seit mehreren Jahren mit TYPO3, nutzen das CMS-System aber nur selten. Große Teile der rund 2.000 Accounts sind nur gelegentlich aktiv und betreuen sehr kleine Inhaltsmengen.Dadurch entsteht eine Situation, in der Erfahrung zwar vorhanden ist, die notwendige Routine jedoch fehlt. Das führt dazu, dass Aufgaben grundsätzlich bekannt sind, aber häufig Unsicherheiten bestehen und Arbeitsschritte länger dauern als nötig. Die Mehrheit bewertet den eigenen Umgang mit der Technik zwar als mäßig sicher bis eher sicher, doch es gibt einen spürbaren Anteil an Personen, die sich im Umgang mit dem System unsicher fühlen. Wirklich hohe Sicherheit ist nur in einer kleinen Gruppe vorhanden. Gleichzeitig zeigt sich im Zeitaufwand für einfache Aktualisierungen, dass viele Nutzende mehr Zeit benötigen als zu erwarten wäre – ein Hinweis auf fehlende Routine, unklare Arbeitsschritte oder mangelnde Systemkenntnis.

Insgesamt entsteht das Bild einer stark dezentralen Redaktion mit sehr heterogenem Kompetenzniveau. Viele Beteiligte arbeiten nur sporadisch, was Unsicherheiten verstärkt und Support sowie Qualitätssicherung erschwert.

3. Neukonzeption des Berechtigungsmodell

Zugangsberechtigungen berühren immer Fragen von Sicherheit und gesetzlichen Vorgaben, weil festgelegt wird, wer *was* im System darf. Eine **Qualifizierung** mindert Risiken durch Fehlbedienungen, Wissenslücken und sicherheitskritisches Verhalten. Zukünftig soll daher der Zugang zum Typo3-System an eine sicherheitsorientierte Qualifizierung gekoppelt sein.

Definiert werden drei Berechtigungsstufen:

3.1. Berechtigungsstufe 1: Inhaltsbearbeitung (niedriges Risiko)

Beschreibung:
Diese Stufe umfasst Personen, die ausschließlich **einzelne Inhalte auf bestehenden Seiten bearbeiten** dürfen. Sie greifen nur in bereits angelegte Strukturen ein und haben keinen Einfluss auf die Navigation oder die Seitenarchitektur. Die Verantwortung dieser Gruppe liegt auf der inhaltlichen Pflege im vordefinierten Rahmen, ohne Eingriffe in technische oder strukturelle Bereiche.

Zulässige Aktionen:

- Texte bearbeiten und aktualisieren
- Bilder austauschen oder ergänzen
- Dateien hochladen und verlinken
- Inhalte innerhalb einer bestehenden Seite neu anordnen
- Metadaten einzelner Inhalte pflegen

Nicht zulässige Aktionen:

- Keine Erstellung, Löschung oder Verschiebung von Seiten
- Keine Änderungen an Navigationsstrukturen
- Keine Nutzung von Plugins

Risikoprofil:
Diese Stufe ist mit einem **geringen Risiko** verbunden, da Fehler auf die Ebene einzelner Inhalte begrenzt bleiben und keine sicherheits- oder strukturrelevanten Auswirkungen haben. Haftungsrisiken sind minimal, sofern grundlegende Standards (z. B. Barrierefreiheit, Urheberrecht) eingehalten werden.

3.2. Berechtigungsstufe 2: Struktur- und Seitenverantwortung (mittleres Risiko)

Beschreibung:
Diese Stufe umfasst Personen, die neben der Inhaltsbearbeitung auch für die **Pflege und Weiterentwicklung einzelner, mittelgroßer Webbereiche bis Institutsgröße oder vergleichbar** verantwortlich sind. Sie arbeiten vertiefend an Seitenstrukturen, Navigation, Seiteneigenschaften und erweiterten redaktionellen Elementen. Eingriffe

erfolgen ausschließlich im zugewiesenen Bereich. Das Aufgabenprofil erfordert ein höheres technisches Verständnis sowie ein Bewußtsein für Auswirkungen auf Nutzerführung, Barrierefreiheit und Auffindbarkeit sowie Risiken bezogen auf Datenverlust.

Zulässige Aktionen

- Neue Seiten innerhalb der eigenen Struktur anlegen
- Seiten verschieben, kopieren, ausblenden oder löschen
- Seiteneigenschaften bearbeiten (Titel, Sichtbarkeit, Einstellungen)
- Umgang mit den Plugins News
- Auslesen von Formulardaten
- Übersetzungen

Nicht zulässige Aktionen

- Keinen Einfluss auf Gesamtarchitektur
- Keine Nutzung des Personenplugins
- Kein Aufbau von Formulare
- Keinen Eingriff bei automatischen Übersetzungen

Risikoprofil

Diese Stufe umfasst ein **mittleres Risiko**, da strukturelle Änderungen direkte Auswirkungen auf Nutzerführung, inhaltliche Konsistenz und die Sichtbarkeit der Website haben können. Fehler können ganze Seitenzweige betreffen, sind aber auf den jeweiligen Verantwortungsbereich begrenzt. Sorgfalt, Systemverständnis und ein klares Arbeiten nach vorgegebenen Standards sind daher zwingend erforderlich.

3.3 Berechtigungsstufe 3: Webbereichskoordination (erhöhtes Risiko)

Beschreibung:
Diese Stufe umfasst Personen, die umfassende Verantwortung für große Webstruktur im Sinne von Fachbereichen oder großen Organisationseinheiten übernehmen. Sie gestalten und betreuen komplexere Inhalte, Strukturen sowie das Personen-Plugin und tragen Verantwortung für redaktionelle Qualität (im Rahmen der Möglichkeiten), Struktur und strategische Ausrichtung ihres Bereichs. Aufgrund der erweiterten Rechte und der möglichen Auswirkungen auf ganze Seitenteile gilt diese Stufe als **erhöht risikobehaftet** und setzt eine entsprechend fundierte Qualifizierung voraus.

Zulässige Aktionen

- Datensätze anlegen, bearbeiten und strukturieren
- Komplexe Inhaltselemente nutzen
- Sitemaps und weitere automatisch generierte Feature anlegen und pflegen
- Arbeit mit Plugins
- News-System strukturiert pflegen (Kategorien, Listen, Einzelansichten)
- Formulare mit Powermail erstellen und verwalten

- Plugins (inhaltlich) übersetzen
- Qualitätskriterien für Webauftritte umsetzen und kontrollieren
- Barrierefreiheit sicherstellen (inkl. tiefergehender Aspekte)
- redaktionelle Themen abstimmen, planen und weiterentwickeln
- konsistente Informationsarchitekturen im Bereich pflegen
- Content-Strategien für den eigenen Bereich entwickeln und umsetzen
- KI-Tools reflektiert einsetzen (Chancen & Grenzen beachten)
- rechtliche und qualitätssichernde Standards (z. B. Barrierefreiheit, Datenschutz, Urheberrecht) verbindlich anwenden und überwachen

Nicht zulässige Aktionen

- keine Vergabe oder Verwaltung von Benutzerrechten
- keine Eingriffe in globale System- oder Templateeinstellungen
- keine Veränderungen an hochschulweiten Navigationsstrukturen
- keine administrative Steuerung übergeordneter Plugins oder Systemmodule
- keine systemkritischen Einstellungen (Caching, Konfiguration, technische Anpassungen)

Risikoprofil
Diese Stufe trägt ein **erhöhtes Risiko**, da Entscheidungen Auswirkungen auf ganze Bereiche, Navigationswege, Plugin-Logiken oder informationskritische Inhalte haben. Fehler können großflächige Konsequenzen haben – für Nutzerführung, Barrierefreiheit, Rechtskonformität und Außenwirkung. Personen in dieser Rolle benötigen daher ein **hohes Maß an Sorgfalt**, strukturelles Denken und fundierte Systemkenntnisse.

4. Neukonzeption des Qualifizierungsmodell

Abgeleitet vom Berechtigungsmodell werden drei Qualifizierungskurse zukünftig als Moodle-Selbstlernkurs zur Verfügung stehen:

1. TYPO3-Basiskurs für SeitenbearbeiterInnen
2. TYPO3-Kurs für RedakteurInnen
3. Kurs für WebbereichskoordinatorInnen mit Schwerpunkt Steuerung von Fachbereichswebauftritten

Ergänzt wird das Kurskonzept durch zwei Grundlagenmodule mit dem Themen „Recht & Qualitätsstandards“ sowie „Webverständnis & Hochschulwebauftritt“.

Die Kurse enthalten Theorie- und PraxisanteileDie Stufen 1 und 2 schließen mit einem Wissensquiz und einem Praxisprojekt ab. Im Anschluss erhalten die Absolventen ein entsprechendes Teilnahmezertifikat für die jeweiligte Berechtigungsstufe. Dieses Zertifikat ist die Voraussetzung für die Accountbeantragung.

Teilnehmende des Kurses 3 erarbeiten sich zusätzliches Wissen im entsprechenden Moodle-Kurs und werden von der zentralen Onlineredaktion intensiv begleitet.

Neukonzeption der Accountvergabe**Neue Mitarbeitenden** erhalten nur dann zukünftig Zugang zum System, wenn sie die beiden Grundlagenmodule und den Basiskurs absolviert haben. Die Accountbeantragung erfolgt über ein formularbasierten Genehmigungsprozess. Gleichzeitig greifen die Mechanismen der Kontingentierung (siehe Punkt 6) im Sinne eines Nachrückverfahrens (eine Person erhält in der Regel nur einen Account, wenn eine andere Person ihre Account abgibt)

Accounts sind grundsätzlich Personenbezogen. Sekundäraccounts dürfen nur in begründeten Ausnahmefällen verwendet werden und müssen von der jeweiligen Fachbereichswebkoordination zugewiesen und betreut werden.

Accounts werden grundsätzlich auf maximal zwei Jahre befristet. Für die Weiterführung des Accounts ist eine Lesebestätigung des Update-Bereichs im Typo3-Qualifizierungsprogramm notwendig. Zudem wird erwartet, dass Typo3-Accountberechtigte sich regelmäßig und unaufgefordert im Moodle-Forum für RedakteurInnen informieren.

6. Kontingentierung der Gesamt-Accountanzahl

Eine Begrenzung der Gesamtanzahl der Typo3-Accounts stärkt die Informationssicherheit erheblich: Sie entzieht automatisierten Angriffen und Schadsoftware die Masse an potenziellen Einfallstoren. Vor diesem Hintergrund wird eine strukturell bezogene Accountkontigentierung eingeführt:

Fachbereiche dürfen bis zu zwei Accounts pro Fachgebiete, ein Account pro Institut und bis zu acht Accounts für den Zentralbereich vergeben. Die genannten Obergrenzen stellen das maximale Kontingent dar. Im Sinne einer proaktiven Schadensminimierung und der Reduzierung digitaler Angriffsflächen ist eine Unterschreitung dieser Richtwerte ausdrücklich erwünscht und anzustreben. Die Fachbereiche werden hierzu explizit aufgefordert.

Zentrale Einrichtungen, wissenschaftliche Zentren, Forschungs- und Kompetenzzentren, Abteilungen und Stabsstellen der Hochschulverwaltung und die studentische Selbstverwaltung erhalten bis zu sechs Accounts. Beauftragte und Interessenvertretungen erhalten bis zu zwei Accounts. Auch hier gilt das Ziel der Accountminimierung.

Für die generischen Instanzen Forschung sowie Tagungen und Konferenzen ist explizit keine Accountvergabe vorgesehen. Hierbei wird davon ausgegangen, dass es sich nur um eine Erweiterung des Webbereichs für bereits Accountberechtigte handelt.

7.) Transformationsprozeß

Zentrale Einrichtungen, wissenschaftliche Zentren, Forschungs- und Kompetenzzentren, Abteilungen der Hochschulverwaltung, Zu einem Stichtag werden alle Account „entwertet“ und nur gemeldete Personen erhalten im Anschluss eine Reaktivierung des Accounts. Diese werden in die Stufe der RedakteurInnen eingestuft.

Eine freiwillige Runterstufung auf die Berechtigungsstufe Seitenbearbeitung wird empfohlen bei entsprechender Selbsteinstufung. Bei den reaktivierten Bestandsaccounts werden die Fristen auf 12, 18 und 24 Monate für eine Fortführungsaktivierung gesetzt, um die umfangreiche Ausgangsanzahl der Accounts besser managenen zu können.

8. Evaluation nach der Einführungsphase

Grundsätzlich wird bei den bereits vergebene und neuen Accounts in enger Abstimmung mit den Fachbereichen und Organisationseinheiten darauf hingearbeitet (Selbstschulung, Nachschulungen, Empfehlungen), dass perspektivisch eine gute Passung zwischen Kompetenz und Systemberechtigung entsteht und insbesondere im Umstellungsprozess den operativen Bedürfnissen Rechnung getragen wird. Der Prozess wird daher evaluatorisch mit dem Ziel begleitet, das Schulungsmaterial und das Gesamtverfahren zu prüfen und ggf. anzupassen.

Das Präsidium hat am 17.08.2026 die Neukonzeption des Berechtigungs- und Qualifizierungsmodells für TYPO3 beschlossen (P/91).