Monitoring-Konzept für das CMS TYPO3

0. Begriffe und Vertragsrollen

- **AG (Auftraggeber):** Universität Potsdam, vertreten durch das ZIM.
- **AN (Auftragnehmer):** beauftragte Agentur.
- **Monitoring (Applikationsebene):** Überwachung und Auswertung TYPO3-relevanter Signale (z. B. Logs/Jobs/Frontend-Checks) zur Früherkennung und strukturierten Bearbeitung von Auffälligkeiten/Störungen.
- **TYPO3-Instanzen:** alle vertraglich einbezogenen Produktiv- und Nicht-Produktiv-Umgebungen gemäß Vereinbarung.

1. Zielsetzung und Geltungsbereich

Dieses Monitoring-Konzept regelt die Überwachung der TYPO3-Instanzen der Universität Potsdam auf Applikationsebene durch den AN sowie die Schnittstelle zum AG (ZIM).

Ziele

- Früherkennung applikationsbezogener Störungen (TYPO3, Extensions, Applikationslogs, Jobs/Scheduler, applikationsnahe Integrationen).
- Transparente Kommunikation und dokumentiertes Vorgehen bei Incidents.
- Regelmäßige Berichte zu Stabilität, relevanten Security Advisories und daraus abgeleitetem Handlungsbedarf.

Geltungsbereich

- Alle TYPO3-Instanzen (Produktiv- und definierte Nicht-Produktiv-Umgebungen) nach Vereinbarung.

2. Rollen und Verantwortlichkeiten

AG (ZIM)

- Verantwortet den Betrieb der Infrastruktur/Plattform (z. B. OS, Netzwerk, Storage, DB-Dienst, Webserver/PHP als Plattformkomponenten) außerhalb des hier beschriebenen Monitoring-Umfangs.
- Stellt erforderliche Schnittstellen bereit (Ticketkanal, benannte Ansprechpartner:innen, vereinbarte Zugänge/Log-Views nach Freigabe).
- Wirkt an der Ursachenabgrenzung mit, sofern Infrastruktur/Plattform als Ursache in Betracht kommt.

AN (Agentur)

- Führt das applikationsbezogene Monitoring gemäß Kapitel 3 durch und übernimmt die Erstdiagnose.
- Erstellt und pflegt Tickets inkl. Statuskommunikation an die benannten Ansprechpartner:innen des AG.
- Bewertet relevante TYPO3 Security Advisories (Core/Extensions) und übermittelt eine Empfehlung zum Vorgehen an den AG.
- Führt vereinbarte Maßnahmen im TYPO3-Kontext (z. B. Konfigurationsanpassungen/Extension-Fixes) nach Freigabe und gemäß Leistungsbeschreibung aus.

Abgrenzung

- Bei Verdacht auf Infrastruktur-/Plattformursachen liefert der AN Befunde (Indikatoren, Zeitfenster, Fehlermuster) und übergibt an den AG.
- Der AN ersetzt nicht das Infrastruktur-Monitoring des AG.

3. Umfang des Monitorings (AN)

Der AN überwacht und bewertet mindestens folgende Signale (soweit technisch verfügbar und vertraglich vereinbart):

3.1 Verfügbarkeit und Frontend-Checks (Applikation)

- Regelmäßige Erreichbarkeits- und Basisfunktionschecks definierter URLs/Endpunkte (z. B. Startseite, zentrale Landingpages; optional weitere Endpunkte nach Vereinbarung).
- Dokumentation von Ausfällen/Auffälligkeiten (Zeitpunkt, betroffene Umgebung, Reproduzierbarkeit).

3.2 Fehlerlage (Logs/Exceptions)

- Auswertung applikationsrelevanter Fehlermuster, insbesondere:
  - 5xx-Fehler sowie auffällige 4xx-Anomalien (soweit aussagekräftig),
  - PHP-/TYPO3-Exceptions und kritische Log-Einträge.
- Schwerpunkt auf wiederkehrenden und auswirkungsrelevanten Fehlern (Reduktion von Lograuschen).

3.3 Jobs/Scheduler

- Monitoring der TYPO3-Scheduler-Tasks (Erfolg/Misserfolg, Laufzeiten, Häufigkeit von Fehlstarts).
- Erkennung wiederkehrender Job-Fehler inkl. Hinweis auf mögliche Ursachen auf Applikationsebene (z. B. Konfiguration, Extension, Timeout-Indikatoren).

3.4 Security Advisories (TYPO3 Core/Extensions)

- Regelmäßige Prüfung relevanter Advisories und Abgleich mit eingesetzter Core-Version/Extensions.
- Einstufung der Relevanz (z. B. kritisch/hoch/mittel/niedrig) und Empfehlung zum Vorgehen (Patch/Update/Mitigation/Beobachten).

4. Incident-Kommunikation und Ticketprozess

4.1 Erkennung und Ticketanlage

- Erkennt der AN eine Störung/Auffälligkeit, wird ein Ticket im vereinbarten System erstellt (oder ein bestehendes Ticket übernommen).
- Das Ticket enthält mindestens: Umgebung, Zeitpunkt/Zeitraum, Symptom, erste Befunde (z. B. Fehlercodes, Logauszüge/Referenzen, Check-Ergebnisse), erste Einschätzung (TYPO3 vs. Infrastrukturverdacht) sowie empfohlene nächste Schritte.

4.2 Abgrenzung und Übergabe

- Bei Infrastruktur-/Plattformverdacht: Übergabe an den AG mit allen relevanten Befunden und Eingrenzungshinweisen.
- Bei TYPO3-Ursache im Verantwortungsbereich des AN: Analyse und Bearbeitung gemäß Leistungsbeschreibung und Freigabeprozess.

4.3 Statuskommunikation

- Statusupdates erfolgen nachvollziehbar über das Ticket; zusätzliche Kommunikationswege (z. B. E-Mail/Telefon) nur, sofern vertraglich/organisatorisch vereinbart.

4.4 Abschluss

- Ticketabschluss mit: Kurzursache, getroffene Maßnahmen, ggf. Workaround, Präventions-/Verbesserungsempfehlung.