



## ANLAGE 2 DOKUMENTATION UND REPORTING ZU SAIT ZVB-IT STAND: 01.01.2026

### 1. Anforderungen an die Betriebsdokumentation

AN wird während der Erbringung der Leistungen eine ausreichende und für den jeweiligen Kunden verständlich formulierte Dokumentation der betreuten Systeme, Leistungen und Prozesse unter Beachtung der mit AN abgestimmten Anforderungen der SAIT in einem gängigen, geeigneten elektronischen Format erstellen und pflegen; die Anforderungen werden je Service zwischen den Parteien vereinbart. Dokumentationen sind so auszugestalten, dass ein fachkundiger Dritter mit entsprechenden Vorkenntnissen Inhalt, Umfang und Besonderheit der jeweiligen Systeme, Leistungen und Prozesse mit angemessen Aufwand nachvollziehen kann. Zu den Betriebsdokumentationen zählen insbesondere, aber nicht abschließend:

- Betriebshandbücher,
- Problemlösungsdatenbank,
- Asset-Management-Datenbank,
- Servicemanagement-Handbuch,
- Quellcode-Dokumentationen und deren Kommentierung bezogen auf von AN spezifisch für den jeweiligen Kunden entwickelte Software

Die Dokumentationen sind durch AN stets aktuell zu halten und bei Veränderungen zeitnah bzw. spätestens innerhalb von 3 Arbeitstage nach Abschluss des Change zu aktualisieren und in einem von SAIT bestimmten Repository für SAIT zugänglich (Leserecht) abzulegen oder der SAIT in sonstiger abgestimmter Form zu übergeben. Eine Dokumentation ist dann als aktuell anzusehen, wenn diese alle relevanten Changes /Änderungen für die jeweils betreffende Leistung enthält. Die Bereitstellung dieser Dokumentation muss unter Berücksichtigung der Regeln des Vertragswerks im Zusam-

menhang mit den Sicherheits- und Complianceanforderungen erfolgen, damit fremder Zugriff vermieden werden kann.

AN wird die vom AG gestellten Vorlagen für die Betriebsdokumentation verwenden, welche die nachfolgenden Mindestinhalte abbildet, beschreibt und dokumentiert. Abweichungen sind von AN anzuzeigen und von SAIT zu bestätigen.

Anforderungen an die Betriebsdokumentation, sofern für den jeweiligen Service zutreffend:

- Beschreibung des Services
  - o Einsatzzweck (wird von dem jeweiligen Kunden vorgegeben)
  - o Schutzbedarf (wird von dem jeweiligen Kunden vorgegeben)
  - o Auflistung der betroffenen organisatorischen Abteilungen sowie der internen und externen Ansprechpartner (wird von dem jeweiligen Kunden vorgegeben)
  - o Beschreibung der Architektur und des Netzplans inkl. der Systemlandschaft, Datenflussdiagrammen, Kommunikationsmatrix und Schnittstellen
  - o Berichtswesen: Beschreibung der Art des Reportings (z. B. Incident-Reporting, Change-Reporting, etc.) und Zeitraum der Berichterstattung sowie der relevanten Reporting-Daten
  - o Mengengerüst des bereitgestellten Service in gemeinsamer Abstimmung mit der dem jeweiligen Kunden (erwartete Nutzerzahl, Datenmengen, Datendurchsatz, etc.)
  - o Grundsätzliche Betriebsanforderungen und Servicequalitäten nach Kundenvorgabe (Verfügbarkeit, Wiederherstellungszeit, Servicezeit, Wartungsfenster, Anforderungen an Datenschutz und Datensicherheit, etc.)
- Installations- und Konfigurationsvorgaben
  - o Installation von Hard- und Software
  - o Konfiguration
  - o Einbindung in Softwareverteilung

- Betriebstätigkeiten
  - Administrationszugänge für die jeweiligen Kunden und Dritte
  - Benutzerrollen und Rechteprofile nach Kundenvorgabe
  - Wartung von Hardware, Betriebssystem, Datenbank und Middleware der Server
  - Monitoring
  - Datensicherung
  - Archivierung
  - Patchmanagement inkl. Testkonzept
- Wiederanlauf, sofern relevant
  - Nach geplanter Betriebsunterbrechung
  - Nach ungeplanter Betriebsunterbrechung
  - Nach Verlust des Systems
    - Wiederbeschaffung und Aufbau der Hardware
    - Wiederherstellung aus Backup oder neue Installation
    - Funktionstest der Anwendung und Abnahme
- Weitere kundenspezifische Prozeduren, Anpassungen (Customizing) und Konfigurationen

Weitere Details zu Abläufen, Kategorisierungen, Priorisierungen und Dokumentation von Incidents können in der Prozessdokumentation (z.B. im Betriebshandbuch) definiert werden.

## 2. Monitoring und Reporting der Erbringung der Leistungen

SAIT und der AN teilen das gemeinsame Verständnis, dass ein effizientes Reporting zur erfolgreichen Zusammenarbeit beiträgt. AN stellt sicher, dass insbesondere die nachfolgenden Anforderungen der SAIT an das Format, die Häufigkeit und die Technologie des Reportings eingehalten werden.

Die Anforderungen sind derart gestaltet, dass das Reporting sowohl in Bezug auf gegenwärtig nachgefragte als auch zukünftig geforderte Services und Leistungen erfüllt werden kann. AN wird fortlaufend Verbesserungsbedarf für das Reporting untersuchen und SAIT die im Sinne der Ziele des jeweiligen Kunden hilfreichen Änderungen vorschlagen. Erforderliche Änderungsvereinbarungen werden die Vertragsparteien auf entsprechende Aufforderung von SAIT hin schließen.

### 2.1 Grundsätze zu Monitoring und Reporting

In einem monatlich für jeden Vertrag zu erstellenden Report berichtet AN der SAIT über die Erbringung der Leistungen auf Basis des AN-seitigen Monitorings. Dabei gelten folgende Qualitätskriterien:

- Messpunkt ist der Leistungsübergabepunkt gemäß den Vorgaben des jeweiligen Vertrages
- Messkriterien sind die Ausprägungen aller vereinbarten Service Level-Parameter und Leistungskennzahlen / KPIs
- Messmethoden sind die entsprechenden Verfahren gemäß den vereinbarten Vorgaben
- Es ist durch AN eine automatisierte Datenerhebung durch ein Monitoring-System am Leistungsübergabepunkt durchzuführen. Eine manuelle Datenerhebung kann in Einzelfällen durchgeführt werden; dies muss jedoch SAIT angezeigt werden und in den Reports gekennzeichnet sein.

AN betreibt und/oder nutzt auf Kundenanforderung Monitoring-Lösungen Dritter und schafft die diesbezüglichen Voraussetzungen, sofern die Monitoring-Lösung so eingeschränkt werden kann, dass ausschließlich kundeneigene Daten einsehbar sind und den Vereinbarungen an die Informationssicherheit entsprechen; in diesem Falle sind die vereinbarten Service Level weiterhin gültig. Im Falle einer Implementierung einer solchen Monitoring-Lösung trägt SAIT die dem AN dadurch tatsächlich entstehenden, nachgewiesenen Aufwände.

Trends und Entwicklungen zu Vergütung, Mengen, Qualitäten und den Service-Level-Parametern müssen erkennbar sein und graphisch dargestellt werden (mindestens hinsichtlich des letzten Reporting-Zeitraums, der letzten 3 (drei) Monate und der letzten 12 (zwölf) Monate).

Die Reports sind durch AN spätestens am 3. (dritten) Arbeitstag nach Stichtag des Berichtszeitraums (Monat) SAIT sowohl in einem zu Microsoft Office kompatiblen Format und in einem geeigneten Dashboard zur Einsicht zur Verfügung zu stellen.

Reports müssen durch AN gemäß den gesetzlichen Anforderungen revisionssicher für mindestens 2 (zwei) Jahre nach Vertragsbeendigung archiviert werden.

Die den Reports zugrundeliegenden Daten werden von AN 180 (einhundertachtzig) Tage nach Lieferung der Reports aufbewahrt; gesetzliche Bestimmungen bleiben hiervon unberührt.

Reports müssen reproduzierbar sein; die Reproduzierbarkeit der Onlinereports aus Rohdaten ist auf 180 (einhundertachtzig) Tage beschränkt. AN stellt dem jeweiligen Kunden auf Verlangen die Rohdaten zur Verfügung und ermöglicht die Einsicht in die Erstellung von Reports anhand der verwendeten

Werkzeuge damit der jeweilige Kunde Reports anhand dieser Rohdaten verifizieren können.

Die Dokumentation der Reporterstellung und -änderung, insbesondere von manuellen Änderungen, ist revisionssicher durchzuführen.

## 2.2 Reportinganforderungen

AN stellt sicher, dass das Reporting mindestens folgende Elemente umfasst:

Report	Detaillierung
Cost reporting	<ul style="list-style-type: none"> <li>- Verdichtete Darstellung der laufenden Vergütung                             <ul style="list-style-type: none"> <li>- pro Vertrag,</li> <li>- pro Monat und Jahr</li> <li>- Fortschreibung der Vergütung pro Jahr bis Vertragsende</li> </ul> </li> <li>- Detailliertes Reporting der laufenden Vergütung                             <ul style="list-style-type: none"> <li>- Menge, Preis</li> <li>- pro Vertrag</li> </ul> </li> <li>- Reporting der aufgelaufenen Einmal-Vergütung (Projekte, Change Requests, optionale Leistungen)                             <ul style="list-style-type: none"> <li>- pro Vertrag</li> <li>- pro Projekt / Change Request</li> <li>- pro Jahr</li> </ul> </li> </ul>
Quality reporting	<ul style="list-style-type: none"> <li>- Reporting der bereits angefallenen, jedoch nicht abgerechneten Leistungen des AN</li> <li>- Darstellung der Service-Level-Treue                             <ul style="list-style-type: none"> <li>- Erfülltes Service-Level</li> <li>- Gefordertes Service-Level</li> <li>- Incidents in kritischen Systemen</li> <li>- SLA-Verletzungen</li> </ul> </li> <li>- IT-Service-Management und Support-Prozesse                             <ul style="list-style-type: none"> <li>- Graphische Darstellung der Entwicklung neu erstellter Tickets pro Thema/Kategorie Ist vs. Soll</li> </ul> </li> <li>- Liste der Tickets mit Laufzeit &gt; 20 (zwanzig) Kalendertage</li> </ul>
Security reporting	<p>Informationen zur Informationssicherheits-Compliance, inklusive, aber nicht abschließend, der folgenden Parameter:</p> <ul style="list-style-type: none"> <li>- Zugriffsberechtigungen auf Anforderung des jeweiligen Kunden, Account-Compliance (insb. Aktualität der Passwörter, begrenzte Rechte, Verstöße gegen Berechtigungskonzept)</li> <li>- Security Incidents                             <ul style="list-style-type: none"> <li>- Security Incidents je Klasse</li> <li>- Nicht fristgemäß behandelte Security Incidents</li> <li>- Reaktionszeit</li> </ul> </li> <li>- Breaches</li> <li>- Abgewehrte Angriffe</li> <li>- Kompromittierte Daten</li> <li>- Spam</li> <li>- Malware</li> <li>- Schwachstellen aus AN-eigenen Quellen (z. B. Scans, Audits):                             <ul style="list-style-type: none"> <li>- gemeldete Schwachstellen</li> <li>- nicht fristgemäß behandelte Schwachstellen</li> <li>- durchschnittliche Bearbeitungszeit Schwachstellen</li> </ul> </li> <li>- Schwachstellen aus Dritt-Quellen (z. B. Hersteller, BSI):                             <ul style="list-style-type: none"> <li>- gemeldete Schwachstellen</li> <li>- nicht fristgemäß behandelte Schwachstellen</li> <li>- durchschnittliche Bearbeitungszeit Schwachstellen</li> </ul> </li> <li>- Patch-Compliance / -Aktualität</li> <li>- Antivirus-Aktualität, -Verfügbarkeit</li> <li>- Nicht fristgemäß umgesetzte Maßnahmen aus einem Audit</li> <li>- Verletzungen der Sicherheitsvorgaben des jeweiligen Kunden</li> <li>- Verletzungen der Sicherheitsvorgaben des AN</li> <li>- Umfang Sicherheitsausgaben für den Vertrag fortlaufend für das Jahr (KPI) gemäß abgestimmter Definition</li> </ul>
Change reporting	<p>Darstellung notwendiger Informationen (Status, Veränderungen, nächste Maßnahmen, Ergebnisse, Planabweichungen in time, in quality, in budget, Risiken) in Bezug auf:</p> <ul style="list-style-type: none"> <li>- Change Requests, zusätzlich auch Post Implementation Reviews</li> </ul>

<b>Report</b>	<b>Detailierung</b>
	<ul style="list-style-type: none"><li>– Wartungen (Planung, Auswirkungen)</li><li>– Patches (Patchstände, Planungen)</li></ul>
Incident reporting	<ul style="list-style-type: none"><li>– Auflistung aller Incidents der im <b>Anlage 1 „Fehlerklassenmodelle“</b> vereinbarten Prioritäten mit ergriffenen Maßnahmen</li><li>– Übersicht der Entwicklung der Incidents nach Prioritäten (Aufkommen, Lösungszeiten, Erstlösungsquote)</li><li>– Auflistung aller offenen Incidents</li><li>– Besondere Ereignisse mit Beeinträchtigung der Service Levels im Incident Management</li><li>– Technische Analyse wichtiger oder sich häufig wiederholender Incidents</li><li>– Vorschläge für Maßnahmen zur künftigen Vermeidung der Incidents</li><li>– Laufende und geplante Maßnahmen zur Verbesserung der Service-Qualität</li></ul>
Problem reporting	<ul style="list-style-type: none"><li>– Auflistung aller Problems der in der <b>Anlage 1 „Fehlerklassenmodelle“</b> vereinbarten Prioritäten und mit besonderer Bedeutung für Availability, Capacity, IT Security Management mit ergriffenen Maßnahmen</li><li>– Übersicht der Entwicklung der Problems nach Prioritäten (Aufkommen, Lösungszeiten, Erstlösungsquote)</li><li>– Auflistung aller offenen Problems</li><li>– Technische Analyse wichtiger oder häufig sich wiederholender Problems</li><li>– Anteil der Workarounds und gelösten Problems</li><li>– Sonstige bedeutende Probleme mit erheblichen Auswirkungen auf die Qualität der Leistungen</li></ul>
Asset reporting	<ul style="list-style-type: none"><li>– Aufstellung aller vertragsgegenständlichen Assets</li><li>– Aufstellung der im Einsatz vor Ort beim AUFTRAGGEBER bzw. beim jeweiligen Kunden befindlichen Geräte</li><li>– Aufstellung der Geräte im Lager</li><li>– Austauschplan der Geräte (Anzahl Geräte pro Monat), Lifecycle-Planung</li></ul>