

EVB-IT Dienstvertrag



Vertragsnummer/Kennung Auftraggeber _____
Vertragsnummer/Kennung Auftragnehmer: V5378/2300000

Seite 1 von 9

Vertrag über die Beschaffung von IT-Dienstleistungen

Zwischen

**Behörde für Schule und Berufsbildung
Hamburger Straße 37
22083 Hamburg**

– im Folgenden „Auftraggeber“ genannt –

und

**Dataport
Anstalt des öffentlichen Rechts
Altenholzer Straße 10 - 14
24161 Altenholz**

– im Folgenden „Auftragnehmer“ genannt –

wird folgender Vertrag geschlossen:

1 Vertragsgegenstand und Vergütung

1.1 Projekt-/Vertragsbezeichnung

Bereitstellung der Infrastruktur und Betrieb des Verfahrens WiBeS im Rechenzentrum sowie technisches Verfahrensmanagement

1.2 Für alle in diesem Vertrag genannten Beträge gilt einheitlich der Euro als Währung.

1.3 Die Leistungen des Auftragnehmers werden

nach Aufwand gemäß Nummer 5.1

zum Festpreis gemäß Nummer 5.2

zuzüglich Reise- und Nebenkosten – soweit in Nummer 5.3 vereinbart – vergütet.

2 Vertragsbestandteile

2.1 Es gelten nacheinander als Vertragsbestandteile:

- dieser Vertrag (Seiten 1 bis 9) mit Anlage(n) Nr. 1, 2a, 2b, 3, 4, 5, 6, 7, 8a, 8b, 9a und 9b, 10
- Allgemeine Vertragsbedingungen von Dataport in der bei Vertragsschluss geltenden Fassung (s. 11.1)
- Dataport Datenschutz-Leitlinie über technische und organisatorische Maßnahmen bei der Datenverarbeitung im Auftrag (s. 11.1)
- Ergänzende Vertragsbedingungen für die Erbringung von IT-Dienstleistungen (EVB-IT Dienstleistung) in der bei Vertragsschluss geltenden Fassung
- Vergabe- und Vertragsordnung für Leistungen – ausgenommen Bauleistungen – Teil B (VOL/B) in der bei Vertragsschluss geltenden Fassung

2.2 Weitere Geschäftsbedingungen sind ausgeschlossen, soweit in diesem Vertrag nichts anderes vereinbart ist.

Vertragsnummer/Kennung Auftraggeber _____

Vertragsnummer/Kennung Auftragnehmer: V5378/2300000

3 Art und Umfang der Dienstleistungen

3.1 Art der Dienstleistungen

Der Auftragnehmer erbringt für den Auftraggeber folgende Dienstleistungen:

- 3.1.1 Beratung
- 3.1.2 Projektleitungsunterstützung
- 3.1.3 Schulung
- 3.1.4 Einführungsunterstützung
- 3.1.5 Betreiberleistungen
- 3.1.6 Benutzerunterstützungsleistungen
- 3.1.7 Providerleistungen ohne Inhaltsverantwortlichkeit
- 3.1.8 sonstige Dienstleistungen: **Bereitstellung der Infrastruktur und Betrieb des Verfahrens WiBeS im Rechenzentrum gem. Anlagen**

3.2 Umfang der Dienstleistungen des Auftragnehmers

3.2.1 Der Umfang der vom Auftragnehmer zu erbringenden Dienstleistungen ergibt sich aus

folgenden Teilen des Angebotes des Auftragnehmers vom

_____ Anlage(n) Nr. _____

der Leistungsbeschreibung des Auftragnehmers

SharePoint Betrieb Motivation und Inhalt	Anlage(n) Nr. 1
kundenspezifische Leistungsbeschreibung	2a
SharePoint Betrieb Leistungsbeschreibung	2b
SharePoint Entwicklung und Beratung Leistungsbeschreibung	3
SharePoint Betrieb Dokumentation Drittanbieterlösungen	4
SharePoint Entwicklung Development Guide	5
AD Leistungsbeschreibung	6
Exchange Leistungsbeschreibung	7
RZ-SLA Teil A	8a
RZ-SLA Teil B	8b
SSLA Teil A	9a
SSLA Teil B	9b

folgenden weiteren Dokumenten:

Leistungsnachweis Dienstleistung _____ Anlage(n) Nr. 10

Es gelten die Dokumente in

obiger Reihenfolge

folgender Reihenfolge: 8b, 8a, 9b, 9a, 2b, 2a, 1, 3, 4, 5, 6, 7, 10

3.2.2 Der Auftragnehmer wird den Auftraggeber auf relevante Veränderungen des Standes der Technik hinweisen, wenn diese für den Auftragnehmer erkennbar maßgeblichen Einfluss auf die Art der Erbringung der vertraglichen Leistungen haben.

3.2.3 Besondere Leistungsanforderungen (z. B. Service-Level-Agreements über Reaktionszeiten):

3.3 Vergütungsbestimmende Faktoren aus dem Bereich des Auftraggebers

Vergütungsbestimmende Faktoren aus dem Bereich des Auftraggebers sind

- a) die Mitwirkungsleistungen des Auftraggebers gemäß Nummer 8
- b) folgende weitere Faktoren:

Vertragsnummer/Kennung Auftraggeber _____
 Vertragsnummer/Kennung Auftragnehmer: V5378/2300000

4 Ort der Dienstleistungen / Leistungszeitraum

4.1 Ort der Dienstleistungen in den Räumlichkeiten des Auftragnehmers

4.2 Zeiträume der Dienstleistungen

Leistungen (gemäß Nummer 3.1)	Geplanter Leistungszeitraum		Verbindlicher Leistungszeitraum	
	Beginn	Ende	Beginn	Ende
Gemäß Nr. 3.1.8 WiBES TEST-Umgebung			01.01.2015	
Gemäß Nr. 3.1.8 WiBES PROD-Umgebung			01.01.2015	
EVB-IT Nr. 5.2 Position 17	01.07.2015			
EVB-IT Nr. 5.2 Position 18	01.12.2015			

4.3 Zeiten der Dienstleistungen

Die Leistungen des Auftragnehmers werden erbracht gemäß SLA RZ Teil A Pkt.4.3, SLA RZ Teil B Pkt.4.1,

4.3.1 während der üblichen Geschäftszeiten des Auftragnehmers an Werktagen (außer an Samstagen und Feiertagen)

_____ bis _____ von _____ bis _____ Uhr
 _____ bis _____ von _____ bis _____ Uhr

4.3.2 während sonstiger Zeiten

_____ bis _____ von _____ bis _____ Uhr
 _____ bis _____ von _____ bis _____ Uhr
 an Sonn- und Feiertagen am Sitz des Auftragnehmers von _____ bis _____ Uhr

5 Vergütung gem. Leistungsnachweis Dienstleistung

5.1



Bezeichnung des Personals/der Leistung (Leistungskategorie)				Preis innerhalb der Zeiten	
Pos. Nr.	SAP-Artikel-Nr.	Artikelbezeichnung/-code	Menge	Mengeinheit	
1	20001062	DP-MSS-STO/SANN; in der Leistung gem. Nr. 5.2 sind 600 Mengeneinheiten enthalten; jede weitere pro Jahr	1	GB/Jahr	
2	20001064	DP-MSS-BACK/30; in der Leistung gem. Nr. 5.2 sind 600 Mengeneinheiten enthalten; jede weitere pro Jahr	1	GB/Jahr	
3	20000139	zusätzliches Exchange Postfach Schüler	1	Stück	
4	20000139	zusätzliches Exchange Postfach Lehrer	1	Stück	
5	20000139	zusätzliche AD-Benutzer (Schüler-Accounts)	1	Stück	
6	20000139	Spamfilter für zusätzliche Postfächer	1	Stück	

EVB-IT Dienstvertrag



Vertragsnummer/Kennung Auftraggeber _____

Vertragsnummer/Kennung Auftragnehmer: V5378/2300000

7	21010345	Restore von Site Collections; Geschätzter Aufwand je 4 Stunden	1	Stunde
8	21010345	Betrieb und Deployment von komplexen Kundenlösungen/Fremdlösungen	1	Stunde
9	21010345	Betriebsleistungen für den authentifizierten Zugriff auf SharePoint	1	Stunde
10	21010345	Sharepoint Beratung und Entwicklung	1	Stunde
11	21010345	Suche im Fileservice oder anderen Anwendungen (je nach Komplexität).	1	Stunde
12	21010347	Consulting – Geschätzter Aufwand 120 Stunden	1	Stunde
13	20000139	CallCenter – geschätzte Incidents 20 Stück pro Monat	1	Stück
14	20000139	2 Jahre gültiges Multidomain SSL Zertifikat wibes.de	1	Stück
15	20000139	2 Jahre gültiges Multidomain SSL Zertifikat wibes-test.de	1	Stück

Die Abrechnung erfolgt nach Aufwand.

Zu Pos. 14 und 15: Die benötigte Menge an SSL-Zertifikaten wird bei der Firma digicert zum Einkaufspreis erworben. Im Verhältnis zwischen Auftraggeber und Auftragnehmer wird einheitlich in Euro abgerechnet. Aufgrund der Tatsache, dass die Zertifikate von Firma digicert in US-Dollar verkauft werden, bestehen Wechselkursrisiken. Entscheidend für die Umrechnung in Euro ist der Kurs am Tag des Einkaufs durch den Auftragnehmer bei Firma digicert."

Rechnungsstellung

Die Rechnungsstellung erfolgt kalendermonatlich nachträglich gem. Leistungsnachweis

Aufwandsbezogene Abrechnungen zu Beginn des Kalenderjahres erfolgen auf Basis der letztmalig zuvor erfolgten Rechnungsstellung vorläufig, falls bereits zuvor Leistungen in Rechnung gestellt wurden. Sofern eine Korrektur der abzurechnenden Mengen erforderlich ist, erfolgt diese mit der darauffolgenden Rechnungsstellung.

Vergütungsvorbehalt

Es wird ein Vergütungsvorbehalt vereinbart

- gemäß Ziffer 6.4 EVB-IT Dienstleistung
 anderweitige Regelung gemäß Anlage Nr. _____

Vertragsnummer/Kennung Auftraggeber _____

Vertragsnummer/Kennung Auftragnehmer: **V5378/2300000**

5.2 Festpreis

Für Lizenzleistungen zahlt der Auftraggeber einen **einmaligen Festpreis** in Höhe von **insgesamt 7.749,76 €**.

Der **einmalige Festpreis** setzt sich wie folgt zusammen:

Pos.	SAP-Artikel-Nr.	Artikelbezeichnung/-code	Menge	Mengen-einheit
1	20000139	SharePoint Server for Internet Sites (TrueUp - SA) Incl. der Lizenzen für Schüler	2	Stück
2	20000139	Einrichtung Domänen (wibes.de;wibes-prod.de;wibes-test.de)	3	Stück
3	20000139	Multidomain SSL Zertifikat wibes-prod.de	1	Stück

Für die vom Auftragnehmer zu erbringenden Dienstleistungen zahlt der Auftraggeber einen **jährlichen Festpreis** in Höhe von **insgesamt € 901.061,59**.

Der **jährliche Festpreis** setzt sich wie folgt zusammen:

Betriebsleistung für die Erweiterung der SharePoint 2010 Infrastruktur

Pos.	SAP-Artikel-Nr.	Artikelbezeichnung/-code	Menge	Mengen-einheit
1	20000139	SharePoint Server for Internet Sites (SA)	2	Service
2	20000139	Virenschutz SharePoint McAfee	1	Stück
3	20000139	Zusätzlicher SharePoint Index/Applikationsserver (Dedicated-XL Premium)	1	Service
4	20000139	Zusätzliches SharePoint Webfrontend (Dedicated-XL Premium)	1	Stück
5	20001062	DP-MSS-STO/SANN Daten Speicher für die Test Umgebung	600	GB
6	20001064	DP-MSS-BACK/30 Backup Speicher für die Test Umgebung	600	GB
7	20000139	eigene DB Instanz	1	Stück
8	20000139	eigener MySite Host	1	Stück
9	21010821	Betrieb SharePoint für die WiBes Anwendung	1	Personen-jahr
10	20000139	Domainregistrierung wibes.de/wibes-test.de/wibes-prod.de	3	Stück je Monat
11	21010345	Betrieb des Applikation Layer Gateway (ALG)	400	Stunde

Vertragsnummer/Kennung Auftraggeber _____

Vertragsnummer/Kennung Auftragnehmer: V5378/2300000

Pos.	SAP-Artikel-Nr.	Artikelbezeichnung/-code	Menge	Mengen-einheit
12	20000139	antellig Stage AppServer (Benutzerverwaltung)	0,5	Service
13	20000139	Prod AppServer (Benutzerverwaltung)	1	Service
14	20000139	Stage AppServer (Web Apps) Server für Bereitstellung der Web Apps in WiBeS TEST	1	Service
15	20001062	DP-MSS-STO/SANN; Daten Speicher für die Stage Umgebung	600	GB
16	20001064	DP-MSS-BACK/30; Backup Speicher für die Stage Umgebung	600	GB
17	20000139	SharePoint LMS – Lizenzkosten 10500 Lizenzen entsprechen 1 Stück	1	Stück / Jahr
18	20000139	SharePoint LMS – Testlizenz 200 Lizenzen entsprechen 1 Stück	1	Stück / Jahr

Betrieb des Active Directory und Exchange

Pos.	SAP-Artikel-Nr.	Artikelbezeichnung/-code	Menge	Mengen-einheit
19	20000139	Exchange Postfach Schüler; 25 MB pro Postfach	7000	Stück
20	20000139	Exchange Postfach Lehrer; 100 MB pro Postfach	3500	Stück
21	20000139	Spamfilter (Postfach)	10500	Stück
22	20000139	AD Benutzer (Schüler-Account)	7000	Stück
23	20000139	AD Benutzer (Lehrer-Account)	3500	Stück

Die Rechnungsstellung des einmaligen Festpreises erfolgt mit Vertragsannahme.

Die Rechnungsstellung des jährlichen Festpreises erfolgt anteilig jeweils zum 1. eines Monats.

Der Auftragnehmer behält sich eine Preisänderung gemäß seinem jeweils gültigen Leistungsverzeichnis vor. Sofern die vorgenannten Preise nicht im Leistungsverzeichnis abgebildet sind, gilt Ziffer 6.4 EVB-IT Dienstleistung.

5.3

Vertragsnummer/Kennung Auftraggeber _____

Vertragsnummer/Kennung Auftragnehmer: V5378/2300000

Seite 7 von 9

6 Rechte an den verkörperten Dienstleistungsergebnissen

(ergänzend zu / abweichend von Ziffer 4 EVB-IT Dienstleistung)

- 6.1 Ergänzend zu Ziffer 4 EVB-IT Dienstleistung ist der Auftraggeber berechtigt, folgenden Dienststellen und Einrichtungen, die seinem Bereich zuzuordnen sind, einfache, nicht übertragbare Nutzungsrechte* an den Dienstleistungsergebnissen einzuräumen:
-
- 6.2 Ergänzend zu Ziffer 4 EVB-IT Dienstleistung ist der Auftraggeber berechtigt, folgenden Dienststellen und Einrichtungen außerhalb seines Bereiches einfache, nicht übertragbare Nutzungsrechte* an den Dienstleistungsergebnissen einzuräumen:
-
- 6.3 Abweichend von Ziffer 4 EVB-IT Dienstleistung räumt der Auftragnehmer dem Auftraggeber das ausschließliche, dauerhafte, unbeschränkte, unwiderrufliche und übertragbare Nutzungsrecht an den Dienstleistungsergebnissen, Zwischenergebnissen und vereinbarungsgemäß bei der Vertragserfüllung erstellten Schulungsunterlagen ein. Dies gilt auch für die Hilfsmittel, die der Auftragnehmer bei der Erbringung der Dienstleistung entwickelt hat. Der Auftragnehmer bleibt zur beliebigen Verwendung der Hilfsmittel und Werkzeuge, die er bei der Erbringung der Dienstleistung verwendet hat, berechtigt.
- 6.4 Sonstige Nutzungsrechtsvereinbarungen
-

7 Verantwortlicher Ansprechpartner

des Auftraggebers:

des Auftragnehmers:

8 Mitwirkungsleistungen des Auftraggebers

- Folgende Mitwirkungsleistungen (z. B. Infrastruktur, Organisation, Personal, Technik, Dokumente) werden vereinbart:
- 8.1 Der Auftraggeber benennt mindestens zwei Mitarbeiterinnen/Mitarbeiter, die dem Auftragnehmer als Ansprechpartnerinnen/Ansprechpartner zur Verfügung stehen.
- 8.2 gemäß Anlage SLA RZ Teil A Anlage 9a Pkt. 2.3, SLA RZ Teil B Anlage 9b Pkt. 2.1, Anlage 2b Punkt 7

9 Schlichtungsverfahren

- Die Anrufung folgender Schlichtungsstelle wird vereinbart:

10 Versicherung

- Der Auftragnehmer weist nach, dass die Haftungshöchstsummen gemäß Ziffer 9.2.1 EVB-IT Dienstleistung durch eine Versicherung abgedeckt sind, die im Rahmen und Umfang einer marktüblichen deutschen Industriehaftpflichtversicherung oder vergleichbaren Versicherung aus einem Mitgliedsstaat der EU entspricht.

Vertragsnummer/Kennung Auftraggeber _____

Vertragsnummer/Kennung Auftragnehmer: V5378/2300000

Seite 8 von 9

11 Sonstige Vereinbarungen

- 11.1. Die Allgemeinen Vertragsbedingungen und die Dataport Datenschutz-Leitlinie sind im Internet unter www.dataport.de veröffentlicht.
- 11.2. Die aus diesem Vertrag seitens des Auftragnehmers zu erbringenden Leistungen unterliegen in Ansehung ihrer Art, des Zwecks und der Person des Auftraggebers zum Zeitpunkt des Vertragsschlusses nicht der Umsatzsteuer. Sollte sich durch Änderungen tatsächlicher oder rechtlicher Art oder durch Festsetzung durch eine Steuerbehörde eine Umsatzsteuerpflicht ergeben und der Auftragnehmer insoweit durch eine Steuerbehörde in Anspruch genommen werden, hat der Auftraggeber dem Auftragnehmer die gezahlte Umsatzsteuer in voller Höhe zu erstatten, ggf. auch rückwirkend.
- 11.3. Die Vertragspartner vereinbaren über die Vertragsinhalte Verschwiegenheit, soweit gesetzliche Bestimmungen wie insbesondere das Hamburgische Transparenzgesetz (HmbTG) dem nicht entgegenstehen.
Unterliegt dieser Vertrag dem HmbTG, so wird er bei Vorliegen der gesetzlichen Voraussetzungen im Informationsregister veröffentlicht. Unabhängig von einer möglichen Veröffentlichung kann der Vertrag Gegenstand von Auskunftsanträgen nach dem HmbTG sein.
- 11.4. Der Auftraggeber kann von diesem Vertrag bis einen Monat nach Veröffentlichung im Informationsregister ohne Angabe von Gründen zurück treten.
Der Auftraggeber verpflichtet sich, unverzüglich nach Vertragsschluss die Veröffentlichung im Informationsregister zu veranlassen und teilt dem Auftragnehmer das Datum der Veröffentlichung mit.
Macht der Auftraggeber vom Rücktrittsrecht Gebrauch, so gilt für den Fall, dass der Auftragnehmer schon vor Ablauf der Rücktrittsfrist mit der Durchführung des Vertrages beginnt, Folgendes:
- Die beiderseits erbrachten Leistungen sind zurück zu gewähren.
 - Ist eine Rückgewähr nicht möglich, so leistet der Auftraggeber Wertersatz.
 - Für die Berechnung des Wertersatzes gelten die in dem Vertrag genannten Leistungsentgelte.
 - Aufwände, für die kein Leistungsentgelt ausgewiesen ist, sind nach dem jeweils gültigen Stundensatz zu vergüten, wenn und soweit sie für die Erfüllung des Vertrages erforderlich waren. Dies gilt vor allem für vorbereitende Tätigkeiten.
 - Für gelieferte Hard- und Software wird das volle Leistungsentgelt erstattet. Verschlechterungen, auch wenn sie durch die bestimmungsgemäße Ingebrauchnahme entstehen, bleiben bei der Wertermittlung außer Betracht. Die Pflicht zum Wertersatz entfällt, soweit der Auftragnehmer die Verschlechterung oder den Untergang zu vertreten hat oder der Schaden gleichfalls bei ihm eingetreten wäre.
 - Hat der Auftragnehmer zur Erfüllung des Vertrages verbindliche Bestellungen bei Lieferanten oder Unterauftragnehmern vorgenommen, die weder storniert noch von dem Auftragnehmer anderweitig verwendet werden können, so nimmt der Auftraggeber die entsprechenden Lieferungen oder Leistungen gegen Zahlung des mit dem Lieferanten oder Unterauftragnehmer vertraglich vereinbarten Preises ab. Dies gilt jedoch dann nicht, wenn sich die Lieferung aus von dem Auftragnehmer zu vertretenden Gründen verschlechtert hat oder untergegangen ist. Der Auftragnehmer setzt sich in jedem Fall nach Kräften für eine Minimierung des Schadens ein.
 - Im Übrigen finden die Bestimmungen der §§ 346 ff BGB entsprechende Anwendung, soweit sich nicht aus den vorstehenden Regelungen etwas anderes ergibt.
- 11.5. Mit diesem Vertrag wird eine etwaige Vorvereinbarung abgelöst. Rechte und Pflichten der Vertragsparteien bestimmen sich ab dem Zeitpunkt seines Wirksamwerdens ausschließlich nach diesem Vertrag.
- 11.6. Rechnungsempfänger für Leistungen aus diesem Vertrag ist die
Behörde für Schule und Berufsbildung
Hamburger Institut für Berufliche Bildung/WiBeS Team
[REDACTED]
Wendenstraße 166
20537 Hamburg
- 11.7. Dieser Vertrag beginnt am 01.01.2015 und gilt für unbestimmte Zeit. Er kann erstmals unter Wahrung einer Frist von 6 Monaten zum 31.12.2016 gekündigt werden. Danach kann er zum Ende eines Kalenderjahres unter Wahrung einer Frist von 3 Monaten gekündigt werden. Die Kündigung bedarf der Textform.

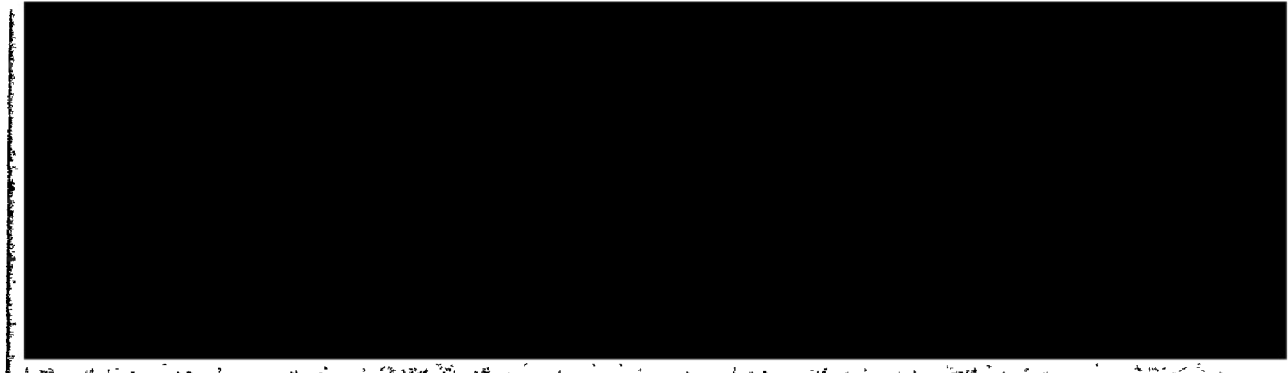
EVB-IT Dienstvertrag



Vertragsnummer/Kennung Auftraggeber _____

Vertragsnummer/Kennung Auftragnehmer: V5378/2300000

Seite 9 von 9



SharePoint Competence Center

Gemeinsame SharePoint Infrastruktur

Motivation und Inhalt

Standardisierter Betrieb von SharePoint SiteCollections und Webanwendungen auf der Standard SharePoint Infrastruktur

Inhaltsverzeichnis

1	Zusammenfassung.....	1
2	Inhalt.....	2
2.1	Anlage 1 SharePoint Betrieb Motivation und Inhalt.....	2
2.2	Anlage 2a kundenspezifische Leistungsbeschreibung.....	2
2.3	Anlage 2b SharePoint Betrieb Leistungsbeschreibung	2
2.4	Anlage 3 SharePoint Entwicklung und Beratung Leistungsbeschreibung	2
2.5	Anlage 4 SharePoint Betrieb Dokumentation Drittanbieterlösungen	2
2.6	Anlage 5 SharePoint Entwicklung Development Guide.....	2
2.7	Anlage 6 AD Leistungsbeschreibung.....	3
2.8	Anlage 7 Exchange Leistungsbeschreibung	3
3	Gründe für eine einheitliche, gemeinsame Infrastruktur	4
3.1	Vorteile und Einsparungen im Betrieb:	4
3.2	Vorteile Geschäftsmodell:.....	4
3.3	Nachteile:	4
4	Gründe für eine standardisierte Infrastruktur	5
4.1	Vorteile im Betrieb	5
4.2	Nachteile	5



1 Zusammenfassung

Für Dataport und Trägerländer wird eine standardisierte SharePoint Umgebung für die Themenfelder

- Zusammenarbeit
- Workflows
- Fachverfahren
- Suche
- Intranetauftritte und Internetauftritte

zur Verfügung gestellt. Zugriffe können aus dem Intranet oder aus dem Internet erfolgen.

Die einzelnen Kundengruppen werden als Mandanten im SharePoint getrennt. Die Trennung geschieht in der Regel über separate Web-Anwendungen.

Die Farm wird standardisiert mit nur geringen Anpassungen betrieben um den kostengünstigen und sicheren Betrieb zu gewährleisten. Für das Deployment von Eigenentwicklungen und Drittanbieterlösungen sind Deployment-Prozesse einzuhalten.

2 Inhalt

Die für die standardisierte SharePoint Infrastruktur angebotenen Leistungen werden durch die folgenden Anlagen beschrieben.

2.1 Anlage 1 SharePoint Betrieb Motivation und Inhalt

Motivation für eine zentrale und standardisierte SharePoint Serverfarm.

2.2 Anlage 2a kundenspezifische Leistungsbeschreibung

Kundenspezifische Leistungsbeschreibung für den Betrieb von SharePoint.

2.3 Anlage 2b SharePoint Betrieb Leistungsbeschreibung

Leistungsbeschreibung für den Betrieb einer standardisierten SharePoint Infrastruktur für Dataport und Trägerländer, Regeln für den standardisierten SharePoint Betrieb.

Insbesondere:

- Leistungsbeschreibung für den SharePoint Support
- Beschreibung und Zuweisung der Rollen wie z.B. Fachliche Leitstelle, Technische Leitstelle, der Kompetenzen und der Abstimmungsprozesse

2.4 Anlage 3 SharePoint Entwicklung und Beratung Leistungsbeschreibung

Leistungsbeschreibung für SharePoint Entwicklung und Beratung.

2.5 Anlage 4 SharePoint Betrieb Dokumentation Drittanbieterlösungen

Formular für die Beschreibung von Drittanbieterlösungen, die auf der zentralen Infrastruktur betrieben werden sollen.

2.6 Anlage 5 SharePoint Entwicklung Development Guide

Regeln für die Programmierung von SharePoint Lösungen, die auf der zentralen Infrastruktur betrieben werden sollen.



2.7 Anlage 6 AD Leistungsbeschreibung

Active Directory Betrieb im Rahmen von SharePoint Anwendungen und Lösungen.

2.8 Anlage 7 Exchange Leistungsbeschreibung

Exchange Betrieb im Rahmen von SharePoint Anwendungen und Lösungen.

3 Gründe für eine einheitliche, gemeinsame Infrastruktur

Die Nutzung einer gemeinsamen Infrastruktur hat deutliche Vorteile. Es werden Synergien geschaffen und die Kosten für die einzelnen Kundengruppen damit erheblich gesenkt. Natürlich werden für eine einheitliche Infrastruktur auch größere Abstimmungsprozesse zwischen den Kundengruppen erforderlich. Tendenziell können diese aber ebenso als Vorteil für den ausfallsicheren Betrieb der Serverfarm gesehen werden.

3.1 Vorteile und Einsparungen im Betrieb:

- Betrieb einer stabilen, ausfallsicheren Standardfarm
- Farm kann temporär für Wartungs- und Migrationsarbeiten aufgespalten werden
- Einsparungen bei Hardware, höhere Verfügbarkeit, bessere Auslastung der Hardware
- Konsistentes Betriebsmodell, Einsparungen im Betrieb
- Platz-/Stromeinsparung im Rechenzentrum (RZ)

3.2 Vorteile Geschäftsmodell:

- Ein konsistentes Geschäftsmodell für alle Trägerländer („SharePoint in the cloud“), Infrastruktur muss nicht vorfinanziert werden
- Neue Anwendungsfälle (z.B. Dataport Internet, Wibes, ...) können zeitnah implementiert werden; es müssen keine neuen Infrastrukturen aufgebaut werden
- Nutzung der Anpassungen für Zusammenarbeit und Intranet einer Kundengruppe auch für andere Kunden
- Formulierung von gemeinsamen Sicherheitskonzepten
- Nutzung des Dataport SharePoint Wissens (Betrieb, Entwicklung, Beratung) ohne Notwendigkeit eigener Ressourcen für den AG.
- Klare Strukturen erlauben einen Masterplan für das Gesamtsystem (was kann wann zu welchen Konditionen zur Verfügung gestellt werden?)
- Erweiterte Möglichkeiten der Länder übergreifenden Zusammenarbeit.

3.3 Nachteile:

- Weniger Flexibilität für den einzelnen Kunden
- Abstimmung zwischen den Kundengruppen notwendig

4 Gründe für eine standardisierte Infrastruktur

Auf der Standard Farm wird SharePoint mit nur geringen Anpassungen betrieben. Für komplexe Fachverfahren werden separate Farmen betrieben.

4.1 Vorteile im Betrieb

- Höhere Verfügbarkeit
- Betriebssicherheit der SharePoint Farm hat höchste Priorität, Komplexität von SharePoint wird nicht weiter erhöht, mögliche Fehlerquellen werden reduziert
- Keine Zuständigkeitsprobleme im Supportfall durch mehrere Produkthersteller auf einer Plattform
- Kleine separate SharePoint Umgebungen für Fachanwendungen sind beherrschbarer als eine große Infrastruktur mit einer hohen Anzahl komplexer Anwendungen und Anpassungen

4.2 Nachteile

- Möglicherweise geringerer Integrationsgrad zwischen den Anwendungen bzw. höhere Integrationsaufwände
- Nicht optimale Auslastung der Hardware



Anlage 2a zum Vertrag V5378/2300000

Kundenspezifische Beschreibung Betrieb WiBeS

für die

Behörde für Schule und Berufsbildung
Hamburger Institut für berufliche Bildung (HIBB)
Wendenstraße 166
20537 Hamburg

nachfolgend Auftraggeber

Version 1.8
Vom 26.06.2013

Inhaltsverzeichnis

1	Allgemeine Beschreibung.....	1
1.1	Beschreibung der zu übernehmenden Lösung	1
2	Voraussetzungen	2
2.1	Kundenspezifische Voraussetzungen.....	2
2.1.1	Mengengerüste	2
2.1.2	Zugriffswege und Netzwerkarchitektur.....	3
2.1.3	Architektur und Verzeichnisdienste.....	3
2.1.4	Geplante Strukturierungsmaßnahmen	3
3	Kundenspezifische Erweiterungen der Infrastruktur	4
3.1	Benutzerverwaltung.....	4
3.2	SharePoint LMS	4
3.3	Ablage von Mediendateien	5
3.4	Office Webapps.....	5
3.5	Kundenspezifische Maßnahmen des Zugriffsschutzes - Sicherstellung der Vertraulichkeit ..	5
3.5.1	UAG	6
3.5.2	Zusätzliche Webanwendung für Daten mit erweitertem Schutzbedarf	6
4	Supportprozess für WiBeS	7
5	Anhang 1 Zusammenfassung SLAs	8
5.1	SLA übergreifende Regelungen	8
5.1.1	Wartungsarbeiten	8
5.1.2	Wartungsfenster	8
5.1.3	Service- und Betriebszeiten.....	9
5.2	Störungsmeldungen	9
5.3	Zusammenfassung aus „SLA Infrastrukturdienste im FHHNET“	12
5.3.1	Verfügbarkeit SharePoint Infrastruktur.....	12
5.4	Zusammenfassung WiBeS Anforderungen.....	1
	Datensicherung.....	1
6	Anhang 2 Eskalationsinstanzen	5
6.1	Stufe 1.....	5
6.2	Stufe 2.....	5

1 Allgemeine Beschreibung

WiBeS bedeutet „Wissensmanagement für Berufliche Schulen in Hamburg“ und ist ein Wissensportal für Mitarbeiter und Mitarbeiterinnen, Schüler und Kooperationspartner des Hamburger Instituts für Berufliche Bildung. Zur detaillierten Beschreibung des strategischen Ansatzes wird auf das WiBeS Strategiepapier verwiesen.

Der Betrieb erfolgt auf der Standard SharePoint 2010 Infrastruktur des Auftragnehmers in der Internet Zone.

1.1 Beschreibung der zu übernehmenden Lösung

Das Portal basiert auf Microsoft SharePoint in der Version 2007. Die Lösung ist aus dem Internet zu erreichen und wurde zurzeit von WiBeS selbst betrieben. Die für die Infrastruktur notwendigen Server werden für WiBeS bei der „HanseNet“ gehostet. Den Betrieb übernehmen die Lehrer selbst. Hierfür sind 1,5 Stellen eingeplant. Die WiBeS-Lösung besteht neben den Servern für SharePoint (Webservern, DB-Servern) auch aus mehreren ISA-Servern, Exchange-Servern und einem Domain-Controller mit einem eigenen AD.

2 Voraussetzungen

2.1 Kundenspezifische Voraussetzungen

Es wird von folgenden Voraussetzungen ausgegangen:

- Das vom Auftragnehmer aufgebaute und zentral finanzierte UAG (Unified Access Gateway) kann vom Auftraggeber genutzt werden. Es gelten folgende Bedingungen:
 - Derzeit wird von den unter 2.1.1 angegebenen Mengengerüsten ausgegangen. Übersteigt die Anzahl der im Maximum angemeldeten parallelen Nutzer (max.concurrent-user) 500 Benutzer, kann der Auftraggeber an den Kosten der Infrastruktur beteiligt werden.
 - Die jährlichen Betriebskosten für das UAG sind in der Kostenkalkulation (vgl. EVB-IT) für die angegebene Benutzeranzahl enthalten.
 - Änderungen oder Tests am UAG, die andere Verfahren beeinflussen könnten, dürfen erst nach Zustimmung des Produktverantwortlichen beim Auftragnehmer durchgeführt werden
 - der Auftraggeber entscheidet über die notwendigen Überprüfungen. Änderungen an den Regelsätzen können nach Zustimmung durch den Produktverantwortlichen beim Auftraggeber durchgeführt werden

- Der Betrieb erfolgt in der zentralen SharePoint 2010 Infrastruktur des Auftragnehmers in der Internet Zone (AD, UAG, SharePoint und Exchange).
- Die UAG Infrastruktur steht mit externem AD und Zugriff auf Exchange (über OWA) und SharePoint in der Internet Zone zur Verfügung
- Lösung HIBB-Mitarbeiter, Kooperationspartner und Schüler
 - Benutzerkonten: Externes AD der Internetzone
 - Benutzerverwaltung erfolgt durch Auftraggeber/ Lehrer über die im Rahmen des Migrationsprojektes zu entwickelnden Webservices (Benutzerverwaltung)
 - Postfächer werden in einem Exchange in der Internet Zone vorgehalten
- Der Auftraggeber hat keine Rechte auf AD oder SharePoint Administrationsebene.
- Der Technische Betrieb erfolgt beim Auftragnehmer (AD, Exchange, SharePoint), der fachliche Betrieb (Benutzer verwalten, SharePoint Site Collection Administration, 1st Level Support) erfolgt durch den Auftraggeber
- Die vorhandenen CALs (Forschung und Lehre) sind für die neue Infrastruktur nutzbar. Lizenziert sind alle beschriebenen Nutzer.

2.1.1 Mengengerüste

Stand 11.01.2013 hat WiBeS folgende Mengengerüste:

- SharePoint-Daten: ca. 280 GB (variiert u.a. auf Grund der Größe des Suchindex usw.)
- Ca. 3000 MySites mit einem Datenvolumen von 9,7 GB
- Anzahl Content-Datenbanken auf dem MSSQL-Server: ca. 75
- Anzahl User (ermittelt über die Anzahl Mailboxen im Exchange)
 - HIBB-Mitarbeiter: 4023
 - Schüler, Kooperationspartner: 10784
- In der Altanwendung gibt es 75 Site Collections
- Max. Concurrentuser = 150 (ermittelt in Q3/Q4 2012)

Auf Grund der derzeitigen geringen Zugriffszahlen wird in der Kostenkalkulation von 10.500 Benutzern ausgegangen (3500 HIBB-Mitarbeiter + 7000 Schüler, Kooperationspartner). Ändert sich das Nutzungsverhalten müssen diese Zahlen nach oben angepasst werden. Aufgrund der Komplexität der Exchange-Umgebung müssen mindestens 10.000 Exchange Konten beauftragt werden.

2.1.2 Zugriffswege und Netzwerkarchitektur

WiBeS ist aus dem Internet zu erreichen. Der Zugriff erfolgt über selbstadministrierte PCs.

2.1.3 Architektur und Verzeichnisdienste

Lehrer und Schüler werden im externen AD der Internetzone verwaltet

Der SharePoint Betrieb erfolgt in eigenen Webanwendungen in der SharePoint 2010 Farm in der Internetzone. Diese Farm wird mit mehreren anderen Kunden geteilt.

Für WiBeS wird ein MySite Host zur Verfügung gestellt, der gegen andere Mandanten abgegrenzt ist. Das bedeutet, dass die MySites von WiBeS nicht für andere Mandanten sichtbar sind und umgekehrt.

In der Internet Zone wird eine Exchange 2010 Infrastruktur für WiBeS aufgebaut.

2.1.4 Geplante Strukturierungsmaßnahmen

Auf Grund der neuen Infrastruktur und rechtlicher Vorgaben wird es notwendig sein, den strukturellen Aufbau nach der 1:1 Übernahme anzupassen. Dazu wird eine zweite Webanwendung als Sicherheitszone eingerichtet. Siehe 3.5.2

Hierbei sollte ein möglicher Einsatz des SharePoint LMS (Learning Management System) berücksichtigt werden.

Die notwendigen Strukturen werden mit der Migration vorbereitet und erfolgen sukzessiv nach der Produktivsetzung.

3 Kundenspezifische Erweiterungen der Infrastruktur

Aktuell besteht die Infrastruktur aus zwei Webfrontends und zwei Node-Datenbankcluster. Die produktive Infrastruktur wird um einen Webfrontend Server, einen Applikationsserver und Datenbankspeicher in einer eigenen Datenbankinstanz erweitert.

Damit ist der SharePoint Betrieb für die Anwendung WiBeS in der angenommenen Größenordnung abgedeckt, das Projekt WiBeS entscheidet über die Strukturierung der Webanwendung in Site-Collections und Sites.

Aktuell besteht die Testumgebung aus einem Webfrondend und einem Datenbankserver. Für die Testumgebung nutzt WiBeS die vorhandene Testumgebung. Die Umgebung wird vorerst nur um den entsprechenden Speicher und einen Applikationsserver erweitert.

Das Betriebspersonal für beide Umgebungen wird mit 1 Personenjahr ab Bereitstellung der Server in Rechnung gestellt.

Die Aufwände werden jährlich überprüft und im Bedarfsfall angepasst. Die Abrechnung erfolgt ab Bereitstellung der Infrastruktur (Server und Speicher). Für den SharePoint-Bereich von WiBeS ist die fachliche Leitstelle SharePoint (FHHportal) zuständig. Hierbei handelt es sich nicht um eine fachliche Leitstelle der fachlichen Anwendung WiBeS.

Vgl. Anlage 2b SharePoint Betrieb Leistungsbeschreibung.docx- Kapitel 5.3 Zuständigkeiten der Fachlichen Leitstelle des Kunden

3.1 Benutzerverwaltung

Für den Auftraggeber ist eine webbasierte Benutzerverwaltung bereitgestellt.

3.2 SharePoint LMS

SharePoint LMS (Learning Management System) ist eine Erweiterung der SharePoint-Infrastruktur, um eine Dritt-Anbieter-Komponente.

Die Installation erfolgt gemäß Anlage 4 SharePoint Betrieb Dokumentation Drittanbieterlösungen.docx

Die jährlichen Lizenzen für das LMS sind in der Kostenkalkulation (vgl. EVB-IT) für die angegebene Benutzeranzahl enthalten. Für die Lizenzbeschaffung ist der Auftragnehmer zuständig. Der Auftraggeber übermittelt die erforderliche Benutzeranzahl an den Auftragnehmer. Eine Inbetriebnahme in der produktiven Umgebung ist nach erfolgreicher Migration zu Auftragnehmer vorgesehen.

3.3 Ablage von Mediendateien

Innerhalb der SharePoint-Infrastruktur werden Mediendateien bisher in den Inhalts-Datenbanken gespeichert. Im Zuge der Migration soll eine geeignetere Form gefunden werden, um Mediendateien abzulegen.

Mögliche Varianten:

- Eine zusätzliche Sitecollection für Medien pro Schule
- Eine globale Sitecollection für Medien für alle Schulen

Eine Inbetriebnahme in der produktiven Umgebung kann nach erfolgreicher Migration zum Auftragnehmer erfolgen.

3.4 Office Webapps

Es ist technisch möglich die Office Webapps zur Verfügung zu stellen. Folgende Bedingungen müssen beachtet werden:

- Lizenzen zum Einsatz von Office Webapps werden durch WiBeS erbracht.
- Die Bereitstellung erfolgt pro Webanwendung.

3.5 Kundenspezifische Maßnahmen des Zugriffsschutzes - Sicherstellung der Vertraulichkeit

Der Auftraggeber hat festgelegt, dass der Standardzugriff (z.B. Schüler) über UAG erfolgt. Der Auftraggeber legt die vorzunehmenden Schutzmaßnahmen fest.

3.5.1 UAG

Der Zugriff auf SharePoint und Exchange erfolgt grundsätzlich über UAG.

Vgl. Anlage 2b SharePoint Betrieb Leistungsbeschreibung - Kapitel: 4.3 Unified Access Gateway (UAG)

Die notwendigen Regeln müssen vom AG definiert werden. Regeln können nur auf Clients mit Windows-Betriebssystem mit Internet Explorer angewendet werden.

Definierbare UAG-Regeln sind u.a.:

- Eine von UAG anerkannte Firewall muss auf dem Client installiert/aktiviert sein
- Aktueller Patchstand eines von UAG anerkannten Virens scanners
- Aktueller Patchstand eines von UAG anerkannten Betriebssystems

3.5.2 Zusätzliche Webanwendung für Daten mit erweitertem Schutzbedarf

WiBeS steht eine zweite Webanwendung zur Verfügung, um Daten mit zusätzlichen Schutzmaßnahmen zu sichern.

Vgl. Anlage 2b SharePoint Betrieb Leistungsbeschreibung - Kapitel: 3.1.4 Webanwendung

Durch eine zweite Webanwendung können weitere Schutzmaßnahmen (z.B. Anpassung People Picker) bereitgestellt werden.

Vgl. Anlage 2b SharePoint Betrieb Leistungsbeschreibung- Kapitel: 4.6.2 Trennung durch separate Webanwendungen

Definierbare Schutzmaßnahmen sind u.a.:

- Anpassung des People Pickers (Auswahl auf Lehrer-Accounts beschränken)
- UAG-Prüfung auf Lehrer-Accounts (separate Zugriffsregeln im AD, die vom Auftraggeber definiert werden)
- SSL-Verschlüsselung
- Erweiterte Erstellung von Log-Dateien
- Regelmäßige automatisierte Überprüfung der Zugriffsberechtigungen
- Kennzeichnung der Sitecollection in der URL

4 Supportprozess für WiBeS

Fragen und Probleme von Schülern und Lehrern werden an die WiBeS-Betreuer der Schulen und die WiBeS Administratoren der BSB/HIBB gemeldet und von diesen als 1st und 2nd Level Support vorgefiltert. Die Gruppen TI41 (AD Verzeichnisdienste), TI42 (Exchange) und TI43 (SharePoint) beim Auftragnehmer stehen als 3rd Level Support bereit. Probleme werden von benannten WiBeS Administratoren über das Call-Center (Mo-Fr von 6.30 Uhr bis 18.00 Uhr (040) 42846 – 750 vom Auftragnehmer gemeldet. Das Call-Center leitet die aufgenommene Störung an die entsprechenden Fachabteilungen weiter.

Aufträge werden von den WiBeS Administratoren über das Auftragspostfach Dataport WiBeS Kundenbetreuung (wibes@dataport.de) gestellt. Diese werden in den Servicezeiten bearbeitet.

Es gelten die Bedingungen aus dem Dokument „Anlage 2b SharePoint Betrieb Leistungsbeschreibung.docx“.

Die Leistungen des Call-Centers für Endbenutzer werden nicht benötigt. Da der Zugriff über selbstadministrierte PCs erfolgt, kann kein Client-Support gewährleistet werden. Es werden lediglich Hilfestellungen zur Problemlösung gegeben und technische Informationen zu den eingesetzten Systemen bereitgestellt.

5 Anhang 1 Zusammenfassung SLAs

Dieses Kapitel dient als Zusammenfassung der gültigen SLAs und Vereinbarungen mit dem Auftraggeber. Es wird dabei auf die jeweils gültigen Dokumente verwiesen.

5.1 SLA übergreifende Regelungen

Zusammenfassung aus „SLA Übergreifende Regelungen“

Vgl.: V5553 Anlage 1 SLA Übergreifende Regelungen v1.docx (Stand 13.08.2012)

5.1.1 Wartungsarbeiten

Wartungsarbeiten, die zu einer Beeinträchtigung des Dialogverkehrs mit den Auftraggeber führen, werden außerhalb der Dialogzeiten durchgeführt. Beim Auftragnehmer gibt es ein extra definiertes Wartungsfenster dienstags, ab 19:00 Uhr - 24:00 Uhr. Das Wartungsfenster wird dem Auftraggeber per Mail und/oder sowie im SCCportal schriftlich angekündigt. Ansonsten erfolgen die Arbeiten nach Absprache mit den betroffenen fachlichen Leitstellen.

Vgl. Anlage 2b SharePoint Betrieb Leistungsbeschreibung -Kapitel 5.13 Wartungsarbeiten

5.1.2 Wartungsfenster

Die Umgebungen WiBeS PROD/TEST werden analog zu den Umgebungen des FHHportals gewartet. Eine Stage-Umgebung für WiBeS ist nicht vorgesehen.

Produktion (WiBeS PROD)

Die Installation von Solutions oder Features, das Einbinden von InfoPath-Formularen sowie vergleichbare Anpassungen in der Produktion erfolgen jeweils am zweiten Dienstag im Monat ab 19:00 Uhr. Softwareupdates erfolgen aufgrund der Installationsdauer an im Einzelfall zu vereinbarenden Wochenenden.

Das Deployment in die Produktion muss bis Freitag Dienstschluss mit allen o.a. Unterlagen beauftragt sein, damit der Change durchgeführt werden kann.

Integration (WiBeS TEST)

In der Integrationsumgebung findet ein wöchentliches Deployment am Donnerstag statt. Das Deployment muss bis Dienstag Dienstschluss mit allen o.a. Unterlagen beauftragt sein, ansonsten verschiebt sich die Installation auf das nächste Wartungsfenster. Am Mittwoch bis 14 Uhr erfolgt durch den Betrieb die Prüfung der Solution und der Dokumentation mit anschließenden Feedback an den Entwickler.

	Integration (WiBeS TEST)	Stage (nicht vorhanden)	Produktion (WiBeS PROD)
Abgabefrist	Dienstag Dienstschluss	Freitag Dienstschluss*	Freitag Dienstschluss*

Wartungsfenster | jeden Donnerstag | jeden Dienstag | jeder 2. Dienstag im Monat

* eine Lösung muss mindestens eine Woche in Integration bzw. Stage getestet werden, bevor ein Antrag für das Folgesystem gestellt werden darf.
(Abweichungen und nähere Details werden in den Ankündigungen veröffentlicht.)

Vgl. Anlage 2b SharePoint Betrieb Leistungsbeschreibung -Kapitel 5.18.7 Termine und Betriebszeiten für Deployments

5.1.3 Service- und Betriebszeiten

Es gelten einheitlich folgende Service- und Betriebszeiten:

Servicezeiten	Montag - Donnerstag	Freitag	Samstag/Sonntag
Annahme/Steuerung von SSRs, SRs	08:00 – 17:00 Uhr	08:00 – 15:00 Uhr	--
Bearbeitung von SSRs, SRs	08:00 – 17:00 Uhr	08:00 – 15:00 Uhr	--
Bediente Betriebszeit	08:00 – 17:00 Uhr	08:00 – 15:00 Uhr	--

* ausgenommen sind bundeseinheitliche Feiertage sowie der 24. und 31. Dezember.

Eine Erweiterung der Service- und Betriebszeiten ist in Ausnahmefällen (z. B. bei Wahlen) nach vorheriger Absprache möglich.¹ Dauerhafte Erweiterungen sind gesondert zu regeln, s. SLA über Betriebs- und Supportleistungen.

SSR=Standard Service Request (Standardaufträge mit def. Ablauf)

SR=Service Request

5.2 Störungsmeldungen

5.2.1.1 Prioritäten

Die Störungsmeldungen werden wie folgt priorisiert:

Dringlichkeit	Kritisch	Kritisch	Kritisch	Hoch	Hoch
	Hoch	Kritisch	Hoch	Hoch	Mittel
	Mittel	Hoch	Hoch	Mittel	Niedrig
	Niedrig	Hoch	Mittel	Niedrig	Niedrig
Auswirkung	Großflächig/ Verbreitet	Erheblich/ Groß	Moderat/ Begrenzt	Gering/ Lokal	

¹ Eine solche Erweiterung bedarf der frühestmöglichen Beantragung über den zuständigen Kundenbetreuer und wird ggf. gesondert berechnet

Die Priorisierung ergibt sich nach der oben abgebildeten Matrix aus den Komponenten Auswirkung und Dringlichkeit. Die Auswirkung bezeichnet den Einfluss, den die Störung auf die geschäftliche Aktivität hat. Die Dringlichkeit einer Störung ist davon abhängig, ob Ersatzwege für die betroffene Tätigkeit möglich sind oder die Tätigkeit zurückgestellt bzw. nachgeholt werden kann. Die Priorität legt die Geschwindigkeiten fest, mit denen die Störung bearbeitet wird und bestimmt die Überwachungsmechanismen:

Priorität	Kritisch	Führt zur umgehenden Bearbeitung durch Dataport und unterliegt einer intensiven Überwachung des Lösungsfortschritts
	Hoch	Führt zur bevorzugten Bearbeitung durch Dataport und unterliegt einer besonderen Überwachung des Lösungsfortschritts.
	Mittel	Führt zur forcierten Bearbeitung durch Dataport und unterliegt der Überwachung des Lösungsfortschritts.
	Niedrig	Führt zur standardmäßigen Bearbeitung durch Dataport und unterliegt der Überwachung des Lösungsfortschritts.

Auswirkung	Geringsfügig	Die Störung betrifft einzelne Benutzer. Die Geschäftstätigkeit ist nicht eingeschränkt.
	Mittlergradig/Begrenzt	Wenige Anwender/Anwenderinnen sind von der Störung betroffen. Geschäftskritische Systeme sind nicht betroffen. Die Geschäftstätigkeit kann mit leichten Einschränkungen aufrechterhalten werden.
	Erschleichend/Groß	Die Geschäftstätigkeit kann eingeschränkt aufrechterhalten werden.
	Großflächig/Verbreitet	Viele Anwender/Anwenderinnen sind betroffen. Geschäftskritische Systeme sind betroffen. Die Geschäftstätigkeit kann nicht aufrechterhalten werden.

Dringlichkeit	Niedrig	Ersatz steht zur Verfügung und kann genutzt werden, oder das betroffene System muss aktuell nicht genutzt werden. Tätigkeiten, deren Durchführung durch die Störung behindert wird, können später durchgeführt werden.
	Mittel	Ersatz steht nicht für alle betroffenen Nutzer zur Verfügung. Die Tätigkeit, bei der die Störung auftrat, kann später oder auf anderem Wege evtl. mit mehr Aufwand durchgeführt werden.
	Hoch	Ersatz steht kurzfristig nicht zur Verfügung. Die Tätigkeit, bei der die Störung auftrat, muss kurzfristig durchgeführt werden.
	Kritisch	Ersatz steht nicht zur Verfügung. Die Tätigkeit, bei der die Störung auftrat, kann nicht verschoben oder anders durchgeführt werden.

5.2.1.2 Reaktionszeiten

Reaktionszeit		
Kennzahl		Leistungsausprägung
Reaktionszeit bei Störungen (während der Servicezeit)	Priorität Kritisch (1)	0,5 Stunden
	Priorität Hoch (2)	1 Stunde
	Priorität Mittel (3)	2 Stunden
	Priorität Niedrig (4)	4 Stunden
	P _{Soll}	90%
	Berichtszeitraum	Kalendermonat

Die Reaktionszeit ist der Zeitraum zwischen der Erfassung der Störungsmeldung und dem Bearbeitungsbeginn (Entgegennahme der weitergeleiteten Störungsmeldung) durch die nachgelagerten Supportinstanzen.

Die Priorität setzt sich aus der Dringlichkeit und der Auswirkung einer Störung zusammen).

Vgl. Anlage 2b SharePoint Betrieb Leistungsbeschreibung- Kapitel 5.15.4 Reaktionszeiten

Vgl. Anlage 2b SharePoint Betrieb Leistungsbeschreibung- Kapitel 5.15.4 Reaktionszeiten

5.3 Zusammenfassung aus „SLA Infrastrukturdienste im FHHNET“

Vgl. V5553 Anlage 4 SLA Infrastrukturdienste im FHHNet v1.docx (Stand 13.08.2012)

5.3.1 Verfügbarkeit SharePoint Infrastruktur

Kennzahl		Leistungsausprägung
Sharepoint Infra- struktur	P _{Soll}	98%
	Indikatoren	Serverhardware Betriebssysteme Datenbank-Instanzen Cluster Services Web- und Sharepoint-Services
	Berichtszeiträume	Monatlich Jährlich kumuliert

5.4 Zusammenfassung WiBeS Anforderungen

In der Zusammenfassung werden Ablauf, Reaktionszeiten und Kosten für anfallende Tätigkeiten erläutert:

Tätigkeit	Integrationsumgebung WiBeS-Test	Produktionsumgebung WiBeS-Prod
<p>Datensicherung</p> <p>Wiederherstellung SharePoint-Inhalte Wann? Wie oft? Aufbewahrungszeit? Was?</p>	<p>In der Umgebung WIBES TEST Erfolgt keine Sicherung</p>	<p>Gem. 5.9 Sicherung und Recovery</p> <p>„Anlage 2b SharePoint Betrieb Leistungsbeschreibung.docx“</p> <p>„Eine Wiederherstellung wird während der Dialogzeiten nach einem Störfall oder nach einer Beauftragung durchgeführt. Wird das System nach einem Störfall wiederhergestellt, werden die fachlichen Leitstellen hierüber informiert“</p> <p><i>Ablauf:</i> Beauftragung per Email an Servicepostfach: wibes@dataport.de</p> <p><i>Reaktionszeit:</i> Nach 4.2</p> <p><i>Kosten:</i> 5 Rücksicherungen im Jahr sind in Betriebskosten* enthalten. Alle weiteren Rücksicherungen werden nach Preisliste abrechnet</p>
<p>Wiederherstellung (Unterscheidung: Gesamtsystem, Teilsysteme der Farm, Website-sammlungen, Websites, Dokument-Bibliotheken, Mailpostfächer u.ä.)</p>		<p><i>Ablauf:</i> Beauftragung per Email an Servicepostfach: wibes@dataport.de</p> <p><i>Reaktionszeit:</i> Nach 4.2</p> <p><i>Kosten:</i> SharePoint</p>
	<p><i>Ablauf:</i></p>	<p><i>Ablauf:</i></p>

	<p>Beauftragung per Email an Servicepostfach: wibes@dataport.de</p> <p><i>Reaktionszeit:</i> Nach 4.2</p> <p><i>Kosten:</i> In Betriebskosten* enthalten</p>	<p>Beauftragung per Email an Servicepostfach: wibes@dataport.de</p> <p><i>Reaktionszeit:</i> Nach 4.2</p> <p><i>Kosten:</i> In Betriebskosten* enthalten</p>
<ul style="list-style-type: none"> - Zielgruppen pflegen - Benutzerprofildienst pflegen - Gesperrte Datentypen pflegen - Einrichten/Ändern/Löschen einer OU im AD - Websitesammlung erstellen/löschen - Inhaltsbereitstellung (Inhalte einer WSS für eine andere WSS bereitstellen / Seiten zwischen verschiedenen Sitecollection umziehen) - Änderung der Sucheinstellungen - Dienstbereitstellung und -verwaltung - Im AD doppelt angelegten Benutzer bereinigen.(Umgang mit 2 Mailboxen.) 	<p><i>Ablauf:</i> Beauftragung per Email an Servicepostfach: wibes@dataport.de</p> <p>Veränderung mit Change Muss bewertet werden</p> <p><i>Reaktionszeit:</i> Nach 4.2</p> <p><i>Kosten:</i> In Betriebskosten* enthalten</p>	<p><i>Ablauf:</i> Beauftragung per Email an Servicepostfach: wibes@dataport.de</p> <p>Veränderung mit Change Muss bewertet werden</p> <p><i>Reaktionszeit:</i> Nach 4.2</p> <p><i>Kosten:</i> In Betriebskosten* enthalten</p>
- Lösung installieren/deinstallieren	<p><i>Ablauf:</i> Vgl. Anlage 2b SharePoint Betrieb Leistungsbeschreibung- Kapitel 5.18 Deployment und Betrieb von (Kunden)Lösungen</p> <p><i>Reaktionszeit:</i> Vgl. 4.1.2 Wartungsfenster</p> <p><i>Kosten:</i> In Betriebskosten* enthalten</p>	<p><i>Ablauf:</i> Vgl. Anlage 2b SharePoint Betrieb Leistungsbeschreibung- Kapitel 5.18 Deployment und Betrieb von (Kunden)Lösungen</p> <p><i>Reaktionszeit:</i> Vgl. 4.1.2 Wartungsfenster</p> <p><i>Kosten:</i> In Betriebskosten* enthalten</p>
<p>Websitesammlung: Kontingent erhöhen (vorhandene Kontingente bleiben nach Migration bestehen)</p>	<p><i>Ablauf:</i> Beauftragung per Email an Servicepostfach: wibes@dataport.de</p> <p><i>Reaktionszeit:</i> Nach 4.2</p>	<p><i>Ablauf:</i> Beauftragung per Email an Servicepostfach: wibes@dataport.de</p> <p><i>Reaktionszeit:</i> Nach 4.2</p>
Wiederherstellung eines im AD ge-	<i>Ablauf:</i>	<i>Ablauf:</i>

<p>löschten Benutzers</p> <p>Gelöschte Objekte AD wiederherstellen.</p>	<p>Benutzer werden in Lösch-OU verschoben und können durch WiBeS innerhalb von 30 Tagen wiederhergestellt werden.</p> <p><i>Versehentlich gelöschte Gruppen oder Benutzer werden grundsätzlich nicht aus dem Backup wiederhergestellt sondern vom WiBeS neu erstellt (entsprechend der Richtlinien des Auftragnehmers)</i></p> <p><i>Eine Ausnahme bilden Vorfälle bei denen die Neu-Erstellung einen unverhältnismäßig hohen Aufwand gegenüber dem Restore darstellen würde. z.B. es würde der der OU Pfad „WIBES“ gelöscht.</i></p> <p>Reaktionszeit: -</p> <p>Kosten: -</p>	<p>Benutzer werden in Lösch-OU verschoben und können durch den Auftraggeber innerhalb von 30 Tagen wiederhergestellt werden.</p> <p><i>Versehentlich gelöschte Gruppen oder Benutzer werden grundsätzlich nicht aus dem Backup wiederhergestellt sondern vom Auftraggeber neu erstellt (entsprechend der Richtlinien des Auftragnehmers)</i></p> <p><i>Eine Ausnahme bilden Vorfälle bei denen die Neu-Erstellung einen unverhältnismäßig hohen Aufwand gegenüber dem Restore darstellen würde. z.B. es würde der der OU Pfad „WIBES“ gelöscht.</i></p> <p>Reaktionszeit: -</p> <p>Kosten: -</p>
<p>User-Massenimport</p>	<p>Erfolgt grundsätzlich über die Benutzerverwaltung durch den Auftraggeber selbst. Darüber hinausgehende Funktionen durch Beauftragung per Email an Servicepostfach: wibes@dataport.de</p> <p>Reaktionszeit: Nach 4.2</p> <p>Kosten: In Betriebskosten* enthalten</p>	<p>Erfolgt grundsätzlich über die Benutzerverwaltung durch den Auftraggeber selbst. Darüber hinausgehende Funktionen durch Beauftragung per Email an Servicepostfach: wibes@dataport.de</p> <p>Reaktionszeit: Nach 4.2</p> <p>Kosten: In Betriebskosten* enthalten</p>
<p>Umgang mit den neuen Mail-Accounts und Zugriff auf die alten Mailkonten-Inhalten</p>	<p>-kein Inhaltsmigration in die TEST-Umgebung -alte Mail-Adressen werden nicht übernommen.</p>	<p>-alte Mail-Adressen werden nicht übernommen.</p>
<p>Web Analytics-Berichte übermitteln</p>	<p>Standard-Webanalytics-Berichte stehen zur Verfügung</p>	<p>Standard-Webanalytics-Berichte stehen zur Verfügung</p>
<p>AD-Report bereitstellen</p>	<p>Ablauf: Per Job wird alle 7 Tage eine .csv mit den geforderten Informa-</p>	<p>Ablauf: Per Job wird alle 7 Tage eine .csv mit den geforderten Informationen</p>

	tionen in eine SharePoint-Bibliothek geschrieben Kosten: In Betriebskosten enthalten	in eine SharePoint-Bibliothek geschrieben Kosten: In Betriebskosten enthalten
--	--	---

***bei erhöhten Aufwand werden die jährlichen Betriebskosten neu berechnet**

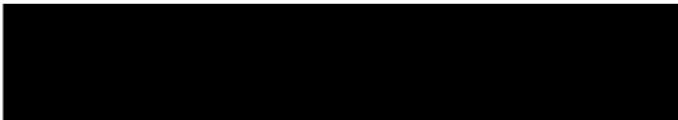
6 Anhang 2 Eskalationsinstanzen

Für eine Eskalation werden folgende Personen benannt:

6.1 Stufe 1



6.2 Stufe 2





Anlage 2b zum Vertrag V5378/2300000

SharePoint Competence Center

SharePoint Betrieb Leistungsbeschreibung

**Betrieb von SharePoint SiteCollections und Webanwendungen
auf der Standard SharePoint Infrastruktur
- Allgemeiner Teil -**

Version 1.8
Vom 26.06.2013

Inhaltsverzeichnis

1	Allgemeine Beschreibung.....	1
1.1	Zugriffsszenarien.....	1
1.2	Mandantenkonzept.....	2
2	Voraussetzungen und Annahmen	3
2.1	CALS.....	3
2.2	UAG und Internetzone.....	3
2.2.1	Zugriffsmöglichkeiten.....	3
2.3	Benutzerkontenverwaltung	4
2.3.1	Interne Benutzer mit Benutzerkonto im FHHNetz	4
2.3.2	Interne Benutzer mit Benutzerkonto im Landesnetz SH.....	4
2.3.3	Externe Benutzer mit Benutzerkonto in der Internetzone	4
2.4	Komponenten der logischen Architektur	4
2.4.1	Serverfarmen.....	4
2.4.2	Dienstanwendungen.....	5
2.4.3	Anwendungspools	5
2.4.4	Webanwendung	5
2.4.5	Inhaltsdatenbank	5
2.4.6	Websitesammlung	5
2.5	Funktionen von SharePoint Server	6
2.5.1	Dokumentmanagement	6
2.5.2	Knowledgemanagement.....	6
2.5.3	Workflows.....	6
2.5.4	Suche.....	7
2.5.5	Content Management.....	7
2.5.6	Taxonomien.....	7
2.5.7	Papierkorb.....	7
3	SharePoint Server Infrastruktur.....	7
3.1	SharePoint Farm im Intranet.....	8
3.2	Produktion	10
3.3	Stage.....	11
3.4	Integration	11
3.5	Test.....	11
3.6	SharePoint Farm in der Internet Zone	12
3.6.1	Produktion	12
3.6.2	Entwicklung	12
3.7	Unified Access Gateway (UAG).....	14
3.8	Anonyme Inhalte (Internetauftritte)	14
3.9	SharePoint Rollen und Komponenten.....	15
3.9.1	Rolle Webserver	15
3.9.2	Rolle Suchserver	15
3.9.3	Rolle Indexierung und Applikationsserver.....	15
3.10	Architektur mit mehreren Anwendungen (Mandanten).....	16

3.10.1	Trennung durch Site Collections	16
3.10.2	Trennung durch separate Webanwendungen	17
3.10.3	Trennung durch eine separate SharePoint Farm	17
3.10.4	Trennung der Datenhaltung auf Datenbankserverseite	17
3.10.5	MySites	18
4	Services und Betrieb der SharePoint Infrastruktur	19
4.1	Zuständigkeiten Dataport SharePoint Betrieb	19
4.2	Zuständigkeiten technische Leitstelle SharePoint Betrieb	19
4.3	Zuständigkeiten der Fachliche Leitstelle des Kunden	20
4.4	Zuständigkeiten fachliche Webanwendungsadministratoren des Kunden	20
4.5	Zuständigkeiten Websitesammlungsadministratoren des Kunden	20
4.6	Grenzen, Beschränkungen und Best Practices	21
4.7	Berechtigungen von Benutzern im SharePoint des Kunden	21
4.8	Datenspeicher	21
4.9	Sicherung und Recovery	22
4.10	Monitoring	22
4.11	Pflege der Software	22
4.12	Patche und Hotfixe	22
4.13	Wartungsarbeiten	23
4.14	Supportprozess für Kunden aus dem Landesnetz SH	23
4.15	Supportprozess für FHH BASIS Kunden	23
4.15.1	Incident Prozess	23
4.15.2	Ticket Priorisierung	24
4.15.3	Ticket Dokumentation in Remedy	26
4.15.4	Reaktionszeiten	26
4.15.5	1st Level UHD Dataport	26
4.15.6	2nd Level: Benutzerunterstützung BASIS	27
4.15.7	2 nd / 3 rd Level: Sharepoint Competence Center – Betrieb	27
4.16	Changemanagement	27
4.16.1	Changes mit Zustimmung bei Vertragsabschluss	28
4.16.2	Changes mit Zustimmung im Einzelfall	28
4.17	SharePoint Designer	28
4.18	Deployment und Betrieb von (Kunden)Lösungen	29
4.18.1	Allgemeine Regeln und Grundsätze	29
4.18.2	Klassifizierung von Anpassungen	29
4.18.3	Lösungsentwicklung	31
4.18.4	Regeln für Lösungsentwicklung	32
4.18.5	Paketierung und Installation	36
4.18.6	Deployment und Freigabeprozess	37
4.18.7	Termine und Betriebszeiten für Deployments	38
4.18.8	Sandboxed Solutions	39
4.19	Unterstützung bei Fragen zur Sicherheitskonzept, Datenschutz und Berechtigungen	39
5	Servicezeiten und Support	40
6	Mitwirkung des Auftraggebers	41

6.1	Webanwendungsadministratoren	41
6.2	Websitesammlungsadministratoren.....	41
6.3	Schutzbedarfeinstufung.....	41
7	Anhang	42
7.1	Dokumentation	42



1 Allgemeine Beschreibung

Für die Unterstützung der übergreifenden Zusammenarbeit mit mehreren verschiedenen Organisationen bietet Microsoft mit dem SharePoint Server eine Arbeitsplattform. SharePoint eignet sich zum Aufbau einfacher, aber auch komplexer Inter-/Intranetportale, sowie zur strukturierten Dokumentablage. Anders als im klassischen File-System werden Dokumente in SharePoint Server mit Metadaten klassifiziert. Dank der umfangreichen Suchfunktion können Informationen unternehmensweit gefunden werden.

Der Betrieb von SharePoint erfolgt auf einer standardisierten SharePoint Server Infrastruktur für alle Trägerländer von Dataport bestehend aus folgenden Komponenten:

- SharePoint Farm im Intranet
- SharePoint Farm in der Internet Zone (für anonyme Zugriffe)
- Zugriffe aus dem Internet auf beide Infrastrukturen über Unified Access Gateway (UAG)

Auf dieser zentralen Infrastruktur wird SharePoint mit geringen Anpassungen betrieben, es wird ein hoher Standardisierungsgrad und größtmögliche Betriebssicherheit angestrebt. Für komplexe Anwendungen mit hohem Anpassungsgrad von Drittherstellern werden separate Infrastrukturen betrieben.

1.1 Zugriffsszenarien

Die Veröffentlichung fokussiert sich dabei momentan auf zwei unterschiedliche Zugriffsszenarien, die nachfolgend beschrieben sind.

Anonymisierter Zugriff:

Es ist beabsichtigt, einzelne Web Seiten über das UAG nach extern (Internet) zu veröffentlichen, die keine Autorisierung des anfragenden Benutzers benötigen. Hierbei handelt es sich um Inhalte für die Allgemeinheit. Es wird sichergestellt, dass die Inhalte so veröffentlicht werden, dass sie vor externen Angriffen sicher sind und keinerlei Auswirkung auf interne Dienste haben.

Personalisierter Zugriff:

Hierbei werden Inhalte veröffentlicht, auf die der Zugriff ausschließlich über eine Autorisierung an einem Benutzer Repository erfolgt. Dabei werden anfragende PC-Systeme lokale Sicherheitsüberprüfungen durchlaufen und je nach Ergebnis unterschiedliche Rechte im Zugriff erhalten (Zustandskontrolle).



1.2 Mandantenkonzept

Die unterschiedlichen Kundengruppen - derzeit FHHportal, Dataport Portal, ShonSh Testportal - werden als einzelne Mandanten voneinander getrennt:

- Je Kundengruppe gibt es eine Webanwendung (Mandant) mit einem Sponsor, der Administratoren und ggf. eine Fachliche Leitstelle stellt oder sich einer bestehenden fachlichen Leitstelle anschließt
- Unter der Webanwendung siedeln sich die SiteCollections in der vom Sponsor festgelegten Struktur und Regeln an
- Jeder MySite Host (Webanwendung) hat einen Sponsor, mehrere Kundengruppen können sich einen MySite Host teilen

Die fachlichen Leitstellen der Mandanten stimmen sich in einem Gremium ab.

Dataport stellt mit der Gruppe Inter-/Intranetservices eine technische Leitstelle, die einen sicheren Betrieb der Infrastruktur gewährleistet und für eine Abstimmung der fachlichen Leitstellen in Betriebsbelangen sicherstellt. Ein Gremium bestehend aus fachlichen Leitstellen und technischer Leitstelle tagt 1/2 jährlich.



2 Voraussetzungen und Annahmen

2.1 CALS

Für die Nutzung muss der Kunde über die entsprechenden CALS verfügen, die Lizenzierung erfolgt nicht über die zentrale Infrastruktur.

Bereits vorhandene Lizenzen, sogenannte (Enterprise) CALS, können in der SharePoint Server Infrastruktur verwendet werden.

Für die gegebenenfalls nötige Beschaffung neuer CALS zur Unterstützung neuer SharePoint-Versionen gelten folgende Verpflichtungen für den Auftraggeber:

- SharePoint Versionen 3 Monate nach Ankündigung durch Microsoft zu unterstützen

Werden die Fristen nicht eingehalten, kann die Anwendung nicht mehr in der zentralen Infrastruktur betrieben werden. Ggf. müssen Anwendungen, auf die dies zutrifft, in eigenen SharePoint Farmen betrieben werden. Die Mehrkosten werden dann vom AG getragen.

Microsoft veröffentlicht [hier](#) eine Übersicht über die Lizenzen und die zugehörigen Features.

2.2 UAG und Internetzone

Die Unified Access Gateway (UAG) Infrastruktur steht mit externem Active Directory und Zugriff auf das FHHportal im internen Netz und die SharePoint Server in der Internet Zone zur Verfügung.

Für Zugriffe, die nicht aus dem FHHNetz oder Landesnetz SH kommen, ist ein Durchgriff auf das FHHportal via UAG aus dem Internet möglich. Diesen Zugriff regelt das Projekt ZUVEX. Verantwortlich ist die FB.

2.2.1 Zugriffsmöglichkeiten

Die folgenden Zugriffsmöglichkeiten werden bereits abgedeckt:

- Mitarbeiter der FHH und von Dataport aus dem FHH-Netz
- Mitarbeiter aus dem Landesnetz SH (LN-SH)
- Zugriffe aus dem FHHportal aus dem Internet via ZUVEX.
- Anonyme Zugriffe
 - Internet Auftritte

Folgende Zugriffsmöglichkeiten sind derzeit in Aufbau:

Darüber hinaus sind folgende Szenarien technisch möglich:



- Aus anderen Netzen/ADs aus den Trägerländern über ADFS und Anbindung des Kunden ADs nach entsprechende Freigabe und technischer Umsetzung
- Anonyme Zugriffe
 - Bürgerverfahren (wie EG-DLRG)

2.3 Benutzerkontenverwaltung

Für die Mitarbeit in SharePoint wird ein AD-Benutzerkonto benötigt. Folgende ADs werden von Dataport betrieben:

- Domäne Land SH de
- FHHnet

2.3.1 Interne Benutzer mit Benutzerkonto im FHHNetz

Soweit möglich, obliegt dem Kunden die Benutzerkontenverwaltung. Die Pflege der Benutzer im FHHNetz AD erfolgt über das Hamburger Service Informationssystem (HaSI).

2.3.2 Interne Benutzer mit Benutzerkonto im Landesnetz SH

Die Pflege der Benutzerkonten in der Domäne Land SH de obliegt dem Kunden.

2.3.3 Externe Benutzer mit Benutzerkonto in der Internetzone

Diese Benutzergruppe wird im externen AD der Internetzone geführt.

Die Verwaltung der Benutzerkonten im externen AD liegt beim Kunden. In welcher Form dies geschieht (z.B. über ein SharePoint Webpart), kann von Fall zu Fall unterschiedlich sein und wird separat betrachtet. Sofern Dataport die Pflege der Benutzerkonten für den Kunden übernimmt, wird dies kostenpflichtig beauftragt. SharePoint Server

2.4 Komponenten der logischen Architektur

SharePoint Server besteht aus einer Reihe an logischen Komponenten, die bei der Planung in Bezug auf Quantität, Verwaltung, Ausprägung, Berechtigung und Isolation beachtet werden sollten.

Die in den folgenden Abschnitten angesprochenen Komponenten werden in der TechNet Library von Microsoft ausführlich beschrieben.

2.4.1 Serverfarmen

Eine Serverfarm stellt im Entwurf der SharePoint-Umgebung das Element in der obersten Ebene dar. Die Verwaltung einer Serverfarm obliegt den Mitgliedern der im Rahmen der Installation angelegten Farmadministratorengruppe.



2.4.2 Dienstanwendungen

Eine Dienstanwendung stellt eine Ressource dar, die von mehreren Webanwendungen in einer Farm gemeinsam verwendet werden kann.

Beispiele für Dienstanwendungen sind Access Services, Dokumentkonvertierung, Suchdienst und der verwaltete Metadatendienst. Eine Übersicht findet sich in der [TechNet Library von Microsoft](#).

2.4.3 Anwendungspools

Ein IIS-Anwendungspool ist ein Konfigurationselement, das über einen Arbeitsprozess oder mehrere Arbeitsprozesse verfügt und dem eine oder mehrere Anwendungen zugeordnet werden. Beim Erstellen von Websitesammlungen und Diensten in SharePoint Server wird ein vorhandener Anwendungspool ausgewählt oder ein neuer erstellt.

2.4.4 Webanwendung

Eine Webanwendung besteht aus einer IIS-Website (Internet-Informationdienste), die als logische Einheit für die erstellten Websitesammlungen dient. Bevor eine Websitesammlung erstellt werden kann, muss als erstes eine Webanwendung erstellt werden. Jede Webanwendung wird durch eine andere IIS-Website mit einem eindeutigen oder freigegebenen Anwendungspool dargestellt.

2.4.5 Inhaltsdatenbank

Der gesamte Inhalt einer Webanwendung wird in Inhaltsdatenbanken gespeichert. Auf Websitesammlungsebene können Inhalte auf mehrere Inhaltsdatenbanken verteilt werden. Eine Inhaltsdatenbank kann mehrere Websitesammlungen enthalten. Eine Websitesammlung kann nur in einer Inhaltsdatenbank liegen und nicht auf mehrere Inhaltsdatenbanken verteilt werden. Üblicherweise legen wir für jede Websitesammlung eine Inhaltsdatenbank ein..

2.4.6 Websitesammlung

Eine SharePoint-Websitesammlung ist eine hierarchische Anreihung von Websites, die gemeinsam verwaltet werden können. Websites in einer Websitesammlung haben gemeinsame Merkmale, wie etwa gemeinsame Berechtigungen, Galerien für Vorlagen, Inhalts-Typen und Webparts, und sie teilen in der Regel eine gemeinsame Navigation. Eine Websitesammlung enthält eine einzige Top-Level-Website und eine beliebige Anzahl von Unterseiten, die in einer Hierarchie organisiert sind. Eine Unterwebsite ist eine einzelne SharePoint-Website in einer Websitesammlung. Eine Unterwebsite kann Berechtigungen und die Navigationsstruktur von der übergeordneten Website erben. Diese können aber auch unabhängig davon festgelegt und verwaltet werden. Die Erstellung von Unterseiten



können an die Mitglieder einer Websitesammlung delegiert werden, aber das Erstellen von Websitesammlungen kann nur von einem Service-Administrator durchgeführt werden.

2.5 Funktionen von SharePoint Server

Die Webanwendung mit SiteCollections bzw. die SiteCollection wird als Zusammenarbeits- und Kommunikationsplattform bereitgestellt. Sie bietet u.a. folgende Funktionen:

- Dokumentmanagement über Metadaten
- Knowledgemanagement über Wikis und Blogs
- Bereitstellung von Standardworkflowfunktionen
- Dedizierte Suche über eine eigene Suchdienstanwendung
- Content Management
- Taxonomien

2.5.1 Dokumentmanagement

Dokumente werden in SharePoint-Bibliotheken abgelegt. Anders als im klassischen File-System werden dabei keine hierarchischen Strukturen mit Ordnern angelegt. Die Bibliothek besitzt benutzerdefinierte Spalten, in denen für jedes Dokument Metadaten gepflegt werden, die das Dokument beschreiben. Es können verschiedene Views auf die Dokumente anhand der Metadaten erstellt werden. Darüber hinaus stehen die Metadaten für die Suche nach Dokumenten zur Verfügung.

Die Funktionen des Ein- und Auscheckens, sowie die Versionierung von Dokumenten ermöglichen das gemeinsame Arbeiten an einem Dokument.

2.5.2 Knowledgemanagement

Wikis und Blogs sind Standard-Funktionalitäten von SharePoint. Sie unterstützen das Wissensmanagement innerhalb des Unternehmens. Der Social Network Gedanke von SharePoint berücksichtigt das aktive Mitwirken aller Mitarbeiter an einem unternehmensweiten Informationspool.

2.5.3 Workflows

SharePoint stellt dem Benutzer eine Auswahl an rudimentären Standardworkflows zur Verfügung. Die Workflows bilden Genehmigungsverfahren und das Einholen von Feedback ab. Komplexere Workflows können mit dem SharePoint Designer oder Visual Studio erstellt werden.

Auf Wunsch kann in der Umgebung Nintex Workflow bereitgestellt werden. Der Kunde übernimmt dafür die entsprechenden Lizenzkosten.



2.5.4 Suche

Zum Auffinden der Informationen und Dokumente bietet SharePoint eine Suchdiensteanwendung. In die Suche werden verschiedene Faktoren einbezogen, u.a. Metadaten. Personen können über die SharePoint Personensuche gefunden werden.

In den vorhandenen SharePoint Infrastrukturen wird derzeit kein FAST-Search betrieben.

2.5.5 Content Management

Für die Veröffentlichung von Informationen im Internet oder Intranet stehen in SharePoint funktionale Content-Management-Werkzeuge zur Verfügung. Es werden unterschiedliche Seitenlayouts angeboten. Medien, wie Bilder und Videos können problemlos in die Seiten integriert werden. Die Publikation der Seiten kann mit Workflows gesteuert werden.

2.5.6 Taxonomien

SharePoint stellt eine umfangreiche Terminologiespeicherverwaltung bereit. Parallel zum Content können damit Taxonomien aufgebaut werden. Die in der Taxonomie gespeicherten Ausdrücke können an jeder beliebigen Stelle der Websitesammlung und auch übergreifend zur Verfügung gestellt werden. Im Hintergrund kann somit unabhängig vom Content ein komplettes Wissensnetz abgebildet werden.

2.5.7 Papierkorb

Alle SharePoint Sites sind mit einer „Papierkorb-Funktionalität“ ausgestattet, wodurch die Benutzer Dokumente innerhalb von 30 Tagen nach der Löschung wiederherstellen können.

Übersteigen die Inhalte der „Papierkörbe“ einer SiteCollection 30% des verfügbaren Gesamtspeichervolumens, werden die älteren gelöschten Dateien schon vor Ablauf der 30 Tage bis zur Unterschreitung dieses Grenzwertes endgültig gelöscht.

3 SharePoint Server Infrastruktur

Die Infrastruktur besteht aus folgenden Komponenten:

- SharePoint Farm im Intranet: Primäre SharePoint-Farm für alle authentifizierten Zugriffe von Internen und Externen. Umgebung für Zusammenarbeit, Intranet, Suche, Workflows und Fachanwendungen.
- SharePoint Farm in der Internet Zone:
 - Farm für anonyme Zugriffe, also Internetauftritte und Bürgerverfahren (z.B. Verfahrensklärung ohne Authentifizierung)
 - Farm für ausschließlich externe Benutzer (wie z.B.: Freiwillige Feuerwehren, Lehrer und Schüler)
- Zugriffe aus dem Internet auf beide Infrastrukturen über das MS Produkt Unified Access Gateway (UAG)

Diese Infrastrukturkomponenten werden im Folgenden beschrieben. Die Zugriffsmöglichkeiten aus dem FHHNetz und dem Landesnetz SH befinden sich im Abschnitt 2.2.1

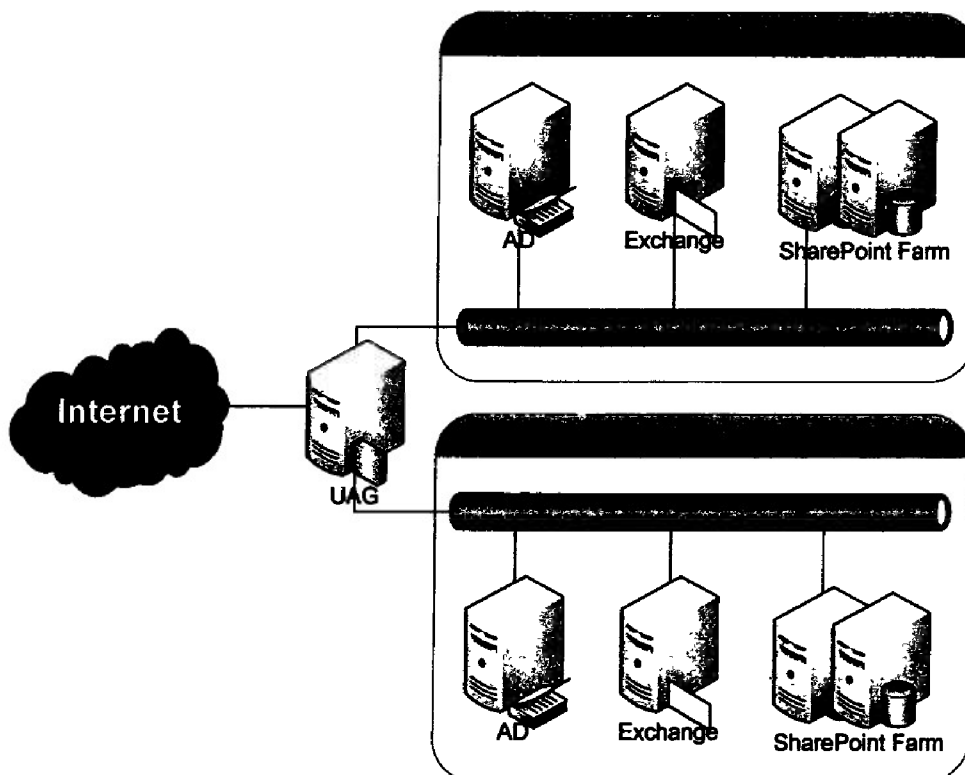


Abbildung 1: Übersicht über die Gesamtinfrastruktur

3.1 SharePoint Farm im Intranet

Die SharePoint Farm im Intranet ist viergliedrig aufgebaut und besteht aus den Umgebungen für die Produktion, Stage (Qualitätssicherung), Integration und Test mit hoher Ausfallsicherheit. Jede einzelne Umgebung besteht wiederum aus einer Datenhaltungskomponente, WebFrontEnd-Servern

(WFE), und Applikationsservern. Darüber hinaus existieren zentrale Systeme für Reporting, PDF-Erstellung und verschiedenen Schnittstellen. Vor jedem System sorgen Hardware Load-Balancer für eine gleichmäßige Lastverteilung auf den dahinterstehenden WFE's.

Dem Auftraggeber (AG) wird eine Standard Microsoft SharePoint Webanwendung mit entsprechenden SiteCollections bzw. einer SiteCollection in der Produktionsumgebung bereitgestellt.

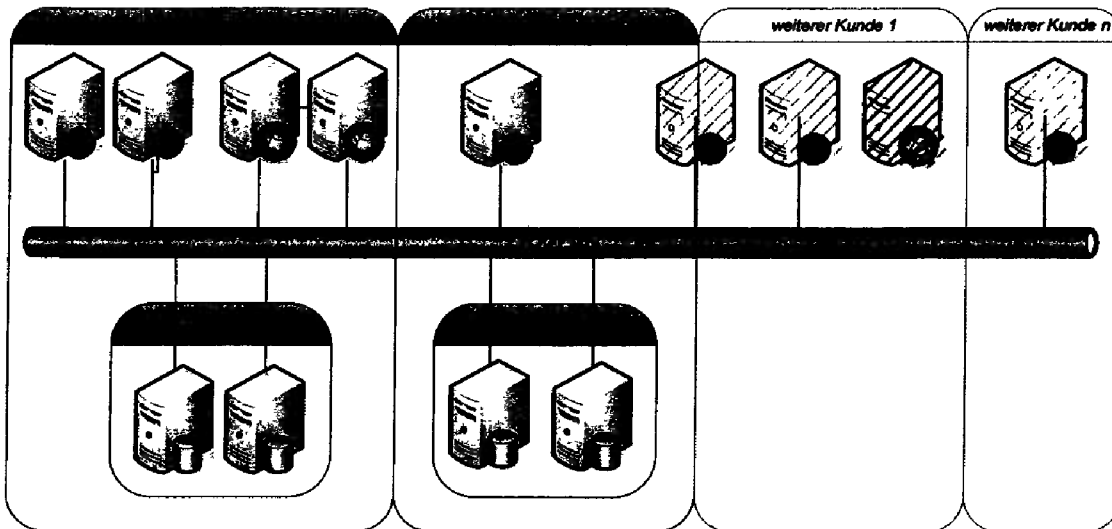


Abbildung 1a: Übersicht Mandantenkonzept

3.2 Produktion

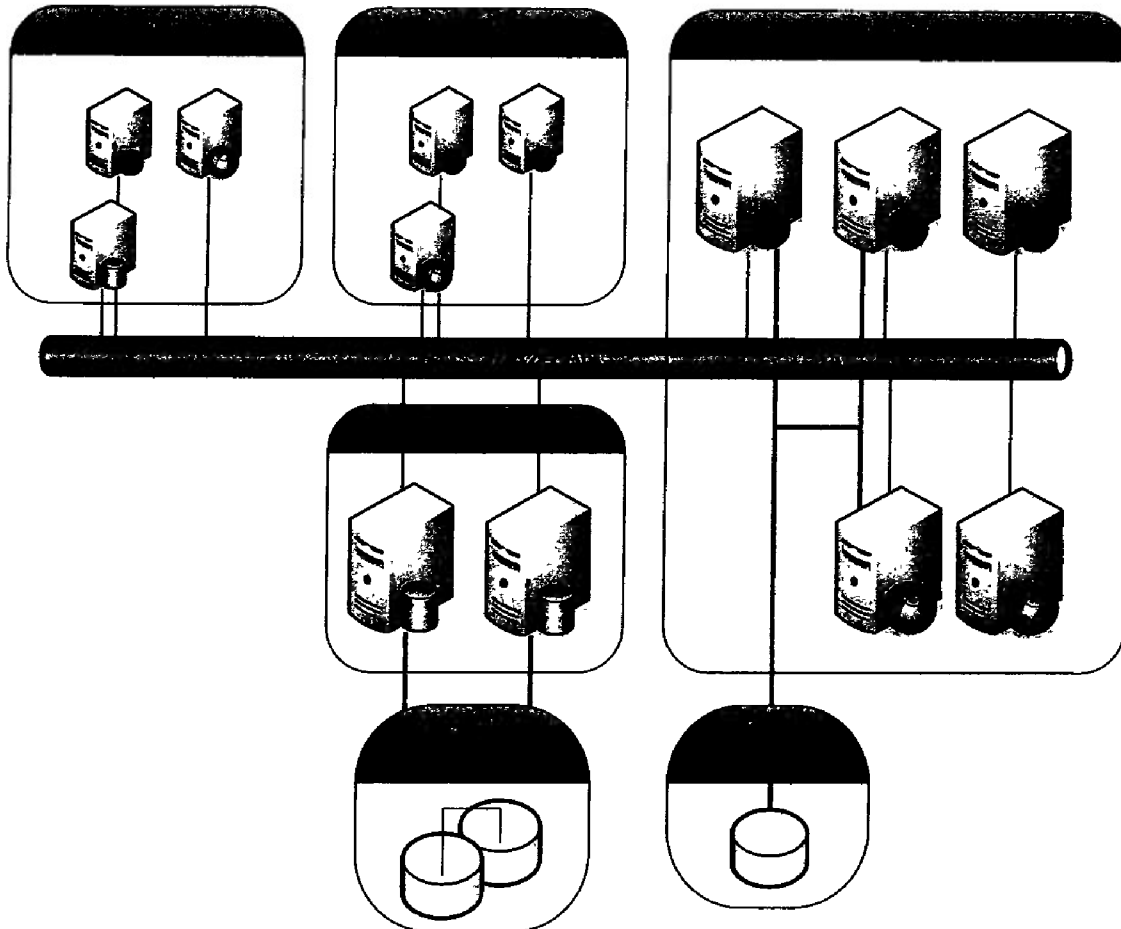


Abbildung 2: Produktionsumgebung der SharePoint Farm

Vier WFE-Server im Load-Balancing sorgen für die Abarbeitung der Kundenanfragen. In der linken Hälfte ist das Datenbanksystem zu sehen. Darüber hinaus existieren zwei Server für die Suchindexierung.



3.3 Stage

Die Stagingumgebung ist das Qualitätssicherungssystem. Jede Softwareversion wird vor der Installation in der Produktion in diesem System abschließend getestet und abgenommen. Nach erfolgter Abnahme durch den Kunden bzw. die technische und die fachliche Leitstelle erfolgt die Verteilung in die Produktion. Die Softwarestände sind bis auf die abzunehmenden Softwareversionen identisch mit denen der Produktion. Im Fehlerfall dient dieses System auch zur Analyse.

Es sind die gleichen Serverrollen wie in der Produktion abgebildet, allerdings nicht in gleicher Anzahl und aus Kostengründen handelt es sich bei den Servern um virtuelle Maschinen. Aus diesem Grund kann man aus dieser Umgebung keine Erkenntnisse über Lastverhalten und Performanceverhalten der Produktionsumgebung gewinnen.

Die Datenhaltung erfolgt in einer separaten Instanz.

3.4 Integration

Die Integration dient der Qualitätssicherung. Jede neue Softwareversion wird vor der Installation in der Produktion in diesem System auf Funktionalität und Verträglichkeit getestet nach erfolgter Abnahme durch den Kunden bzw. die technische und die fachliche Leitstelle erfolgt die Beauftragung für die Abnahme in der Stage und danach der Installation in der Produktion.

Es sind die gleichen Serverrollen wie in der Produktion und Stage abgebildet, allerdings nicht in gleicher Anzahl und aus Kostengründen handelt es sich bei den Servern um virtuelle Maschinen. Aus diesem Grund kann man aus dieser Umgebung keine Erkenntnisse über Lastverhalten und Performanceverhalten der Produktionsumgebung gewinnen.

Die Datenhaltung erfolgt in einer separaten Instanz.

3.5 Test

In der Testumgebung werden Funktionalitäten einzelner Komponenten geprüft sowie Integrationstests durchgeführt. Hier werden auch mal neue Softwarelösungen eingespielt und getestet. Der Deploymentprozeß ist für die Umgebung stark vereinfacht. Eine kurze Beauftragung per Mail reicht für diese Umgebung aus.

Die Umgebung besteht aus drei Maschinen mit den Rollen Web Frontend/Suche und Indexierung/Applikation.

Die Datenhaltung erfolgt auf einer eigenen Instanz.

3.6 SharePoint Farm in der Internet Zone

Die folgende Abbildung beschreibt die Komponenten des SharePoint Servers in der Internet Zone.

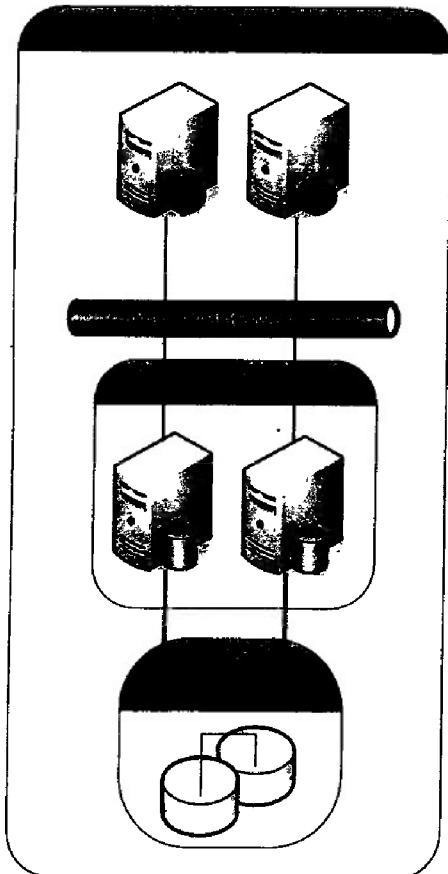


Abbildung 3: Komponenten des SharePoint Servers in der Internet Zone

3.6.1 Produktion

Die Umgebung besteht aus einem DB Cluster mit zwei Knoten und zwei WebFrontEnd Servern und ist damit ausfallsicher ausgelegt.

3.6.2 Entwicklung



Die Umgebung besteht aus einem DB-Server und zwei WebFrontEnd Servern und ist damit ausfallsicher ausgelegt. Der Zugang zum Testen erfolgt wie in der Produktion aus dem Internet heraus.

3.7 Unified Access Gateway (UAG)

Mit dem Aufbau einer UAG Infrastruktur und einer separaten SharePoint Umgebung in der Internetzone werden Zugriffe aus Internet ermöglicht. Mit dieser Lösung können auch anonyme Inhalte (Internetauftritt, Bürgerdienste) zur Verfügung gestellt werden.

Als Lösung und Plattform für die sichere Veröffentlichung und den sicheren Zugriff auf interne Dienste wird das Microsoft Unified Access Gateway eingeführt.

Das UAG ist vorgesehen für eine Veröffentlichung von internen Infrastrukturdiensten über das Internet. Primär sollen folgende Ziele erreicht werden sollen:

- Die sichere Veröffentlichung von internen Infrastrukturdiensten wie der internen SharePoint Infrastruktur
- Eine sicherere Authentifizierung an den Diensten, die eine Authentifizierung verlangen
- Die sichere Veröffentlichung von Diensten, die der Allgemeinheit zur Verfügung gestellt werden (anonym zugreifbare Inhalte)
- Eventuelle Risiken sollen im Rahmen der Veröffentlichungsarchitektur eingeschätzt werden können

Ein Zugriff auf die SharePoint Farm im Intranet ist nicht zulässig.

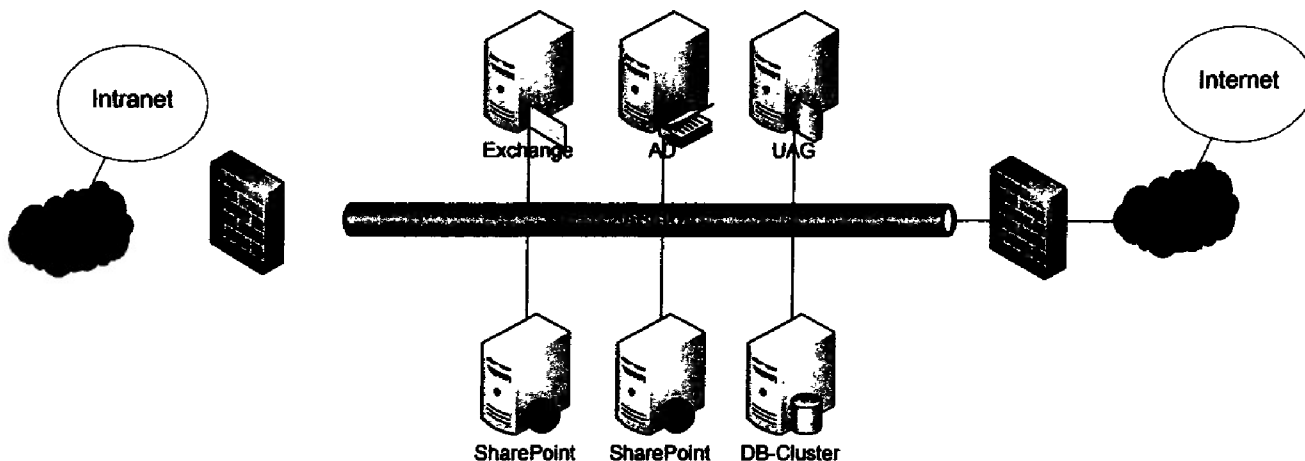


Abbildung 4: Zugang über das UAG

3.8 Anonyme Inhalte (Internetauftritte)

Anonym zugängliche Inhalte wie Internetauftritte oder Bürgerverfahren können zukünftig über eine SharePoint-basierte Lösung implementiert werden. Diese Lösung wird aus infrastruktureller Sicht durch zwei SharePoint-Farmen realisiert. Die interne Farm wird als Redaktionssystem für den

Internetauftritt verwendet, die extern stehende Farm wird für den anonymen Zugriff aus dem Internet auf die veröffentlichten Inhalte verwendet. Damit wird die sog. „Two-farm topology“ implementiert:

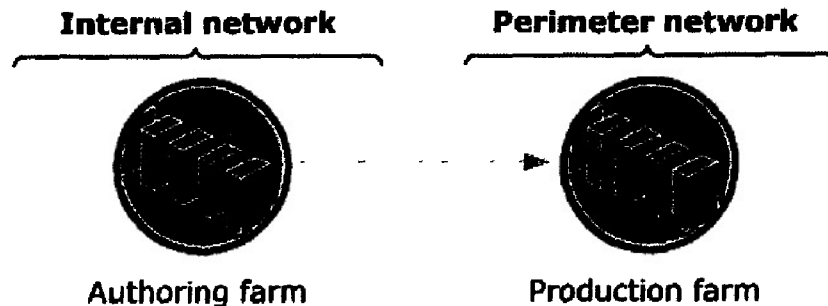


Abbildung 5: Veröffentlichung von Inhalten aus der internen Farm in der externen Farm

Die externe Farm wird innerhalb der Internet Zone von ZABI realisiert und besteht wie beschrieben aus einem Datenbankcluster mit zwei Knoten und zwei WebFrontEnd Servern.

3.9 SharePoint Rollen und Komponenten

3.9.1 Rolle Webserver

Für die Präsentation und für die Bearbeitung der Benutzeranfragen dienen drei Webserver, die über ein NLB (Load-Balancing) Verfahren miteinander verbunden sind. Diese Vorgehensweise unterstützt sowohl die Ausfallsicherheit, als auch die Lastverteilung. Das System lässt sich durch Hinzufügen von weiteren Servern weiter skalieren.

3.9.2 Rolle Suchserver

Die drei Webserver dienen auch als Suchserver, einer weiteren Rolle in der SharePoint Architektur. Die Suchanfragen profitieren ebenfalls vom NLB-Verbund hinsichtlich der Verfügbarkeit und der Lastverteilung. Für die Datenhaltung der Suche verfügt jeder Server über einen größeren Datenspeicher aus dem SAN. Die Daten werden mit den Daten des Indexservers während der Indexierung abgeglichen und dupliziert.

3.9.3 Rolle Indexierung und Applikationsserver

Aus Performancegründen hat man sich für die Rolle Indexierung für zwei dedizierte Maschinen entschieden. Die Datenhaltung für die Indexierung findet lokal auf der Maschine statt. Der Server verfügt über einen größeren Datenspeicher aus dem SAN. Während der Indexierung werden die Daten mit den Daten der Suchserver abgeglichen.



In seiner Rolle als Applikationsserver stellt dieser Server weitere Dienste für die Farm bereit. Das sind insbesondere die Verwaltung der MySite-Funktionalität und die Shared Services der Web-Applikationen.

Die Indizierung von File-Servern muss separat beauftragt und abgerechnet werden. Datenbank
Für die Datenhaltung der im SharePoint entstehenden Daten wird ein MS SQL-Server eingesetzt. Um eine hohe Verfügbarkeit zu gewährleisten, kommen derzeit Clustersysteme mit mindestens zwei Knoten zum Einsatz. Das System verfügt über mehrere DB-Instanzen, die im Normalbetrieb gleichmäßig auf alle Knoten verteilt werden. Kommt es zu einem Ausfall eines Knotens, übernimmt der verbleibende Knoten den Betrieb aller Instanzen.

3.10 Architektur mit mehreren Anwendungen (Mandanten)

Die unterschiedlichen Kundengruppen – derzeit FHHportal, Dataport Portal, ShonSh Testportal – werden durch folgende Maßnahmen voneinander getrennt:

- Trennung der Kundengruppen durch separate Web Anwendungen und ggf. wenn vom Kunden gewünscht eigene Datenbankinstanzen
- Trennung der Kunden im Betrieb (Zentraladministration) mit SharePoint möglich
- Trennung der Services (Suche, Metadaten) nach Kunden /-gruppen
- Trennung der Datenhaltung durch Hosting der Website Collections in eigenen Datenbanken

Der Zugriff auf die Mandanten aus dem Internet über UAG erfolgt nur nach Beauftragung durch den Kunden.

Grundsätzlich gibt es die folgenden Möglichkeiten:

- Trennung durch Site Collections
- Trennung durch separate Webanwendungen
- Trennung durch separate SharePoint Farm

3.10.1 Trennung durch Site Collections

Die Trennung durch Site Collections ist das Standardverfahren innerhalb von Kundengruppen. Die Site Collection repräsentiert die nächstkleinere Einheit innerhalb einer Webanwendung.

- Verwaltung der Site Collection durch eigene Site Administratoren, mit voller Kontrolle über die gesamte Site Collection
- Trennung der Zugriffsrechte zwischen den jeweiligen Kundengruppen, jede Kundengruppe hat nur Zugriff auf die eigene Site Collection.



3.10.2 Trennung durch separate Webanwendungen

Durch eine eigene Webanwendung kann eine Abtrennung auf weiteren Ebenen erfolgen. Die folgenden Aspekte können bei einer Trennung für die jeweiligen Mandanten umgesetzt werden:

- Eigenes Design
- Inhaltsorganisation
- Möglichkeit der Verwendung eines eigenen Application Pools gewährleistet eine höhere Ausfallsicherheit
- Möglichkeit eines eigenen FQDN (Fully qualified domain name), z.B. mein.website-portal.local und der Verwendung von nicht Standard-Ports
- Eigene Dienstanwendungen und Dienstanwendungskonfigurationen
- People Picker kann für Benutzerauswahl teilweise angepasst/gefiltert werden

3.10.3 Trennung durch eine separate SharePoint Farm

Eine SharePoint Server Farm besteht aus min. einem bis zwei Application- / WebFrontEnd -Servern und einem Datenbank-Server (der jedoch auch mit anderen geteilt werden kann – siehe 3.10.4). Zu den vorangegangenen Trennungsmöglichkeiten kommen folgende dazu:

- Vollkommen eigenständige Konfiguration nach Kunden
- Mehrere Webanwendungen möglich
- Nur eigene/benötigte Features
- Eigene Wartungsfenster (Hotfixe, Patchstand, Downtime, etc.) nach Vereinbarung mit dem Kunden
- Komplette Trennung (nur in Verbindung mit eigenem Datenbank Server)

3.10.4 Trennung der Datenhaltung auf Datenbankserverseite

Je nach Anwendungsfall und geforderter (Ausfall-)Sicherheit wird mit dem Kunden die Trennung der Daten auf Datenbankseite vereinbart. Grundsätzlich ergeben sich die folgende Möglichkeiten:

- Vorhalten der Kundengruppendaten einer Site Collection in eigenen Inhaltsdatenbanken
- Trennung der jeweiligen Mandanten durch eine separate Datenbank-Serverinstanz auf demselben Windows-Server. Vorteilen sind die Unabhängig von anderen Datenbank-Serverinstanzen, z.B. bei Wartungsfenstern sowie eigene Wartungspläne für Datenbank-Serverupdates
- Trennung der Mandanten durch einen eigenen Datenbank Server, um eine zusätzliche Unabhängigkeit von Serverwartungen zu gewährleisten und eigene entsprechende Wartungspläne zu einrichten.



3.10.5 MySites

Bezüglich des Einsetzens von MySites gibt es mehrere Möglichkeiten:

- Keine Verwendung der MySites
- Eigener MySite Host (mit oder ohne mandantenabhängiger Zugriffsregulierung)
- Shared MySite Host

3.10.5.1 Keine Verwendung der MySites

Für die Nutzer werden keine MySites bereitgestellt. Die Nutzer können auch auf anderen MySite-Hosts keine eigenen MySites erstellen.

3.10.5.2 Eigener MySite Host

Die Organisation betreibt einen eigenen MySite Host für die eigenen Nutzer. Das Layout kann teilweise angepasst werden, siehe Punkt 3.10.2. Es handelt sich dabei immer um eine eigene Webanwendung. Diese kann mit oder ohne mandantenabhängige Zugriffregulierung erstellt werden. Der Zugriff von organisationsfremden Nutzern kann gesteuert werden und die Bereitstellung als Shared MySite Host ist möglich.

3.10.5.3 Shared MySite Host

Ein Shared MySite Host ist der eigene MySite Host eines sogenannten Sponsors, der diesen finanziert und seiner eigenen und auch fremden Organisationen zur Verfügung stellt. Vereinbarungen über den Umfang der Nutzung des Shared MySite Hosts werden mit dem Sponsor abgesprochen bzw. von ihm vorgegeben und sind in der Regel für alle Nutzer gleich. Alle Nutzergruppen des Shared MySite Hosts haben die gleichen Zugriffsrechte, eine Unterteilung der Zugriffsrechte zwischen diesen Gruppen ist nicht möglich.



4 Services und Betrieb der SharePoint Infrastruktur

4.1 Zuständigkeiten Dataport SharePoint Betrieb

Die SharePoint Infrastruktur wird durch die Gruppe Inter-/Intranetservices bei Dataport betreut. Zu den typischen Leistungen gehören u.a. folgende Tätigkeiten:

- Architektur und technisches Design der Infrastruktur
- Durchführung aller zentralen Administrationsaufgaben
 - Einspielen von Produkt-Updates (wie Service Packs und CUs), inkl. Test; typischerweise gibt es 4-6 größere Updates pro Jahr
 - Problembeseitigung und Kommunikation mit dem Produkthersteller
 - Zuschnitt und Administration der unterliegenden Datenbanken
 - Überwachung der Systeme (automatisiert)
 - Restore von Datenbanken
 - 2nd und 3rd Level Support bei Infrastrukturproblemen in Zusammenarbeit mit User-HelpDesk bzw. CallCenter von Dataport sofern beauftragt bzw. der Supportstruktur des Kunden
- Administration von zentralen SharePoint Anpassungen, wie beispielsweise
 - Deployment von Layout und Design von Masterpages
 - Deployment von Webparts
- Websitesammlungen initial administrieren
 - Erstellen, verändern und löschen von Websitesammlungen
 - Einrichtung und Verwaltung der Userrechte „Site-Owner“
 - Verwalten der Quotas
- Administration der Dienstanwendungen
 - Konfiguration der Suche, Anbindung externer Datenquellen
 - Konfiguration der BI-Basis-Funktionalitäten
 - Administration der Benutzerprofile
- Stellen einer technischen Leitstelle
- Technische Unterstützung der fachlichen Leitstellen bei der Erstellung einer Risikoanalyse

4.2 Zuständigkeiten technische Leitstelle SharePoint Betrieb

Dataport stellt mit dem SharePoint Betrieb eine technische Leitstelle mit folgenden Aufgaben:

- Koordination der fachlichen Leitstellen in einem ¼ jährlich tagendem Gremium
- Entscheidung über die Betreibbarkeit von Anpassungen in der SharePoint Infrastruktur in Abstimmung mit den fachlichen Leitstellen



- Technische Freigabe von Anpassungen und Lösungen, die in der Farm betrieben werden sollen

4.3 Zuständigkeiten der Fachliche Leitstelle des Kunden

Für jede Kundengruppe muss eine Fachliche Leitstelle bestehen. Der AG nennt dem AN zwei Personen, die die Rolle der Fachlichen Leitstelle übernehmen. Aufgaben sind u.a.

- Erstellung einer Risikoanalyse
- Übergeordnete Organisation der Site Collections und Webanwendungen
- Freigabe von Anpassungen und Lösungen, die in der Webanwendung betrieben werden sollen
- Absprache mit den Fachlichen Leitstellen der anderen Kundengruppe und mit dem AN

Eine Fachliche Leitstelle kann mehrere Webanwendungen betreuen.

4.4 Zuständigkeiten fachliche Webanwendungsadministratoren des Kunden

Für jede Kundengruppe muss eine übergreifende Webanwendung bestehen. Der AG nennt dem AN zwei Personen, die die Rolle der Webanwendungsadministratoren übernehmen. Aufgaben sind u.a.

- Übergeordnete Organisation der Site Collections in Abstimmung mit der Fachlichen Leitstelle
- Vergabe von Berechtigungen
- Erster Ansprechpartner für die Endbenutzer und Websitesammlungsadministratoren bei Problemen mit der SharePoint Infrastruktur, Kommunikation mit dem SharePoint Betrieb sofern der UserHelpDesk bzw. das CallCenter von Dataport nicht beauftragt sind.

4.5 Zuständigkeiten Websitesammlungsadministratoren des Kunden

Der AG nennt dem AN zwei Personen, die die Rolle der Websitesammlungsadministratoren übernehmen. Aufgaben der Websitesammlungsadministratoren sind u.a.

- Aufbau der generellen Struktur der Websitesammlung inkl. Navigation
- Vergabe von Berechtigungen
- Aktivieren und Deaktivieren von Websitesammlungsfeatures
- Bereitstellen von Website-Templates
- Erster Ansprechpartner für die Endbenutzer bei Problemen mit der SharePoint Infrastruktur, Kommunikation mit dem Websitesammlungsadministratoren sofern der UserHelpDesk bzw. das CallCenter von Dataport nicht beauftragt sind.



4.6 Grenzen, Beschränkungen und Best Practices

Die vom Hersteller festgelegten Softwarebeschränkungen und -grenzen sind Maximalwerte (<http://technet.microsoft.com/de-de/library/cc262787.aspx>), die in der Praxis jedoch die Kapazitätsauslegung des Systems sehr stark belasten. Um einen performanten Betrieb zu gewährleisten, gelten aus diesem Grund die Best Practices-Grenzen:

Bereich	Grenze	Maximalwert	Best Practices
WebApp	Uploadgröße	2 GB	50 MB (100 MB)
	Inhaltsdatenbank	200 GB	80 GB
WebSiteSammlung	WebSiteSammlung	100 GB	80 GB
Listen / Bibliotheken	Dateigröße	2 GB	50 MB
	Anzahl Dokumente pro Liste	30.000.000	10.000
	Listenelement	30.000.000	10.000
	Anzahl Dokumente pro View	5.000	5.000
	Hauptversionen	400.000	100
	Massenupload	100 Elemente	50 Elemente
Blogs	Blogbeiträge	5.000	5.000
	Blogkommentare	1.000	1.000
Terminologiespeicher	Geschachtelte Ebenen	7	3
	Ausdruckssätze	1.000	100
	Ausdrücke in einem Ausdruckssatz	30.000	10.000
Sicherheit	Anzahl der SP-Gruppen, zu denen ein Benutzer gehören kann	5.000	100
	Benutzer einer WebSiteSammlung	2.000.000	100.000
	SharePoint-Gruppen pro WebSite-Sammlung	10.000	500

4.7 Berechtigungen von Benutzern im SharePoint des Kunden

Die Berechtigung der Benutzer obliegt dem Kunden.

- In der Webanwendung als Webanwendungsadministrator
- In der Websitesammlung als Websitesammlungsadministrator
- In der Website als Besitzer der Website

4.8 Datenspeicher

Die Daten werden in einer Datenbank gespeichert, welche auf dedizierten Datenbankserver betrieben werden.



Die Abrechnung erfolgt automatisiert nach dem beauftragten Volumen.

4.9 Sicherung und Recovery

Die Daten des FHHportal werden täglich gesichert. Auf Anforderungen des Kunden können auch kürzere Abstände der Sicherungsintervalle eingerichtet werden, der dafür erforderliche Mehraufwand wird dem Kunden in Rechnung gestellt. Die Daten werden 30 Tage vorgehalten, es sei denn, der Kunde wünscht andere Aufbewahrungszeiten.

Eine Wiederherstellung wird während der Dialogzeiten nach einem Störfall oder nach einer Beauftragung durchgeführt. Wird das System nach einem Störfall wiederhergestellt, werden die fachlichen Leitstellen hierüber informiert.

4.10 Monitoring

Dataport überwacht die Systeme automatisiert. Kommt es zu Ausfällen oder Engpässen, werden entsprechende Tickets generiert. Während der Dialogzeiten (siehe Abschnitt 5) werden die entstandenen Tickets bearbeitet und das System entstört. Evtl. auftretende Engpässe werden an die fachlichen Leitstellen gemeldet und es werden gemeinsam Maßnahmen eingeleitet, welche die Engpässe beheben.

Eine 7x24 Rufbereitschaft kann beauftragt werden.

4.11 Pflege der Software

Im Windows-Rechenzentrum wird die eingesetzte Basis-Software für das Betriebssystem und andere Serverprodukte der Fa. Microsoft nur solange betrieben, wie diese vom Hersteller gepflegt und unterstützt werden. Im Rahmen der durch Dataport abgeschlossenen Assurance Vereinbarungen werden die Microsoft Server Produkte auf den jeweils aktuellen Versions-Stand gebracht. Die Migrationskosten für das Betriebssystem sind im Serverpreis enthalten. Datenbanken und SharePoint Migration sind eigene Migrationsprojekte und werden gesondert vom Kunden beauftragt.

Aufwände für Anpassungen bei eingesetzter bzw. einzusetzender Server- und Applikationssoftware, die nicht mehr vom Hersteller gepflegt bzw. unterstützt werden, gehen zu Lasten des Kunden.

4.12 Patche und Hotfixe

Bevor neue Software in die Produktion eingespielt wird, wird diese in der entsprechenden Stage/Testumgebung auf Funktionalität und Verträglichkeit getestet. Anschließend erfolgt die Freigabe durch die technische Leitstelle und ggf. die fachliche(n) Leitstelle(n).



Einzige Ausnahme von der Freigabepflicht durch die technische und fachliche Leitstelle betrifft Patches und Hotfixes des Betriebssystems, welche die Sicherheit der Systeme betreffen. Diese werden umgehend auf allen Systemen installiert.

4.13 Wartungsarbeiten

Wartungsarbeiten, die zu einer Beeinträchtigung des Dialogverkehrs mit den Kunden führen, werden außerhalb der Dialogzeiten durchgeführt. Bei Dataport gibt es ein extra definiertes Wartungsfenster dienstags, ab 19:00 Uhr - 24:00 Uhr. Das Wartungsfenster wird dem Kunden per Mail, sowie im SCCportal schriftlich angekündigt. Ansonsten erfolgen die Arbeiten nach Absprache mit den betroffenen fachlichen Leitstellen.

4.14 Supportprozess für Kunden aus dem Landesnetz SH

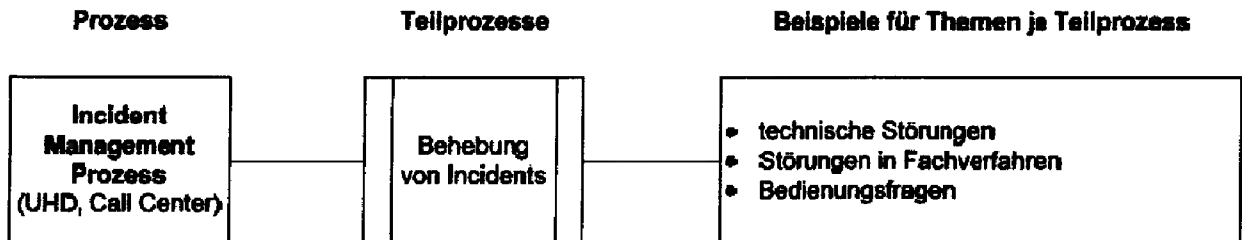
Supportprozesse für Kunden aus dem Landesnetz Schleswig-Holstein sind zurzeit noch nicht beschrieben und beauftragt. Grundsätzlich kann für die Landeskunden am Standort Kiel der Support über das Büro-Land in Betracht gezogen werden. Neben der notwendigen Schulung der Mitarbeiter bedarf es einer vertraglichen Grundlage. Des Weiteren kann selbstverständlich das Call Center Dataports – bei entsprechender Vertragslage – eingebunden werden.

4.15 Supportprozess für FHH BASIS Kunden

In diesem Abschnitt wird der Support Prozess für BASIS Kunden beschrieben. Für alle anderen Kunden kann der Supportprozess bei entsprechender Vertragslage über das Call Center von Dataport erfolgen oder der Kunde stellt 1st und ggf. 2nd Level Support zur Verfügung.

4.15.1 Incident Prozess

Der Incident Management Prozess nach ITIL beinhaltet die schnellstmögliche Behebung von Incidents. Der UHD ist dabei der Ausgangspunkt für den Incident Management Prozess. Daneben werden auch Standard Service Requests bearbeitet. Als Unterscheidung dient die Planbarkeit. Dabei sind Incidents nicht planbare Vorkommnisse wie Störungen oder Fragen zur Bedienung von Anwendungen, während über Service Requests planbare Leistungen abgerufen werden.



Damit Dataport einen Überblick über alle Incidents erhält, wird für jede Störungsmeldung und für jede Kundenanfrage ein Ticket in der zentralen Ticket-Anwendung erstellt. Damit werden die Verfolgung der Bearbeitung und eine Auswertung der Incidents über ein Reporting möglich.

Folgende Aktivitäten beinhaltet die Bearbeitung von Incident Tickets:

1. Störungserkennung und – Registrierung
2. Klassifizierung und erste Unterstützung
3. Untersuchung und Diagnose
4. Behebung und Wiederherstellung
5. Störung schließen
6. Zuständigkeit, Überwachung, Nachverfolgung, Kommunikation

4.15.2 Ticket Priorisierung

Siehe Dokument „Service Level Agreement (SLA) - Übergreifende Services“.

Für Störungsmeldungen steht BASIS-Kunden der User Help Desk (UHD) zur Verfügung. Die Störungsmeldungen von BASIS-Kunden/Anwendern werden wie folgt kategorisiert und bearbeitet:

Dringlichkeit	Kritisch	Kritisch	Kritisch	Hoch	Hoch
	Hoch	Kritisch	Hoch	Hoch	Mittel
	Mittel	Hoch	Hoch	Mittel	Niedrig
	Niedrig	Hoch	Mittel	Niedrig	Niedrig
Auswirkung		Großflächig/ Verbreitet	Erheblich/ Groß	Moderat/ Begrenzt	Gering/ Lokal

Die Priorisierung ergibt sich nach der oben abgebildeten Matrix aus den Komponenten Auswirkung und Dringlichkeit. Die *Auswirkung* bezeichnet den Einfluss, den die Störung auf die geschäftliche Aktivität hat. Die *Dringlichkeit* einer Störung ist davon abhängig, ob Ersatzwege für die betroffene Tätigkeit möglich sind oder die Tätigkeit zurückgestellt bzw. nachgeholt werden kann. Die *Priorität*



legt die Geschwindigkeiten fest, mit denen die Störung bearbeitet wird und bestimmt die Überwachungsmechanismen:

Priorität	Kritisch	Führt zur umgehenden Bearbeitung durch Dataport und unterliegt einer intensiven Überwachung des Lösungsfortschritts
	Hoch	Führt zur bevorzugten Bearbeitung durch Dataport und unterliegt einer besonderen Überwachung des Lösungsfortschritts.
	Mittel	Führt zur forcierten Bearbeitung durch Dataport und unterliegt der Überwachung des Lösungsfortschritts.
	Niedrig	Führt zur standardmäßigen Bearbeitung durch Dataport und unterliegt der Überwachung des Lösungsfortschritts.

Auswirkung	Gering/Lokal	Die Störung betrifft einzelne Benutzer. Die Geschäftstätigkeit ist nicht eingeschränkt.
	Mittel/Begrenzt	Wenige Anwender sind von der Störung betroffen. Geschäftskritische Systeme sind nicht betroffen. Die Geschäftstätigkeit kann mit leichten Einschränkungen aufrechterhalten werden.
	Ersichtlich/Groß	Die Geschäftstätigkeit kann eingeschränkt aufrechterhalten werden.
	Großflächig/Verbreitet	Viele Anwender sind betroffen. Geschäftskritische Systeme sind betroffen. Die Geschäftstätigkeit kann nicht aufrechterhalten werden.

Dringlichkeit	Niedrig	Ersatz steht zur Verfügung und kann genutzt werden, oder das betroffene System muss aktuell nicht genutzt werden. Tätigkeiten, deren Durchführung durch die Störung behindert wird, können später durchgeführt werden.
	Mittel	Ersatz steht nicht für alle betroffenen Nutzer zur Verfügung. Die Tätigkeit, bei der die Störung auftrat, kann später oder auf anderem Wege evtl. mit mehr Aufwand durchgeführt werden.
	Hoch	Ersatz steht kurzfristig nicht zur Verfügung. Die Tätigkeit, bei der die Störung auftrat, muss kurzfristig durchgeführt werden.
	Kritisch	Ersatz steht nicht zur Verfügung. Die Tätigkeit, bei der die Störung auftrat, kann nicht verschoben oder anders durchgeführt werden.



Die Bewertung erfolgt unter Einbeziehung der Einschätzung des Anwenders durch den UHD.

Der Prozess zur Störungsbearbeitung bei Dataport enthält Eskalationsverfahren, die sicherstellen, dass die zugesagten Reaktionszeiten eingehalten werden und dass eine zuverlässige und schnellstmögliche Störungsbearbeitung erfolgt.

Sollte ein Anwender mit der Priorisierung sowie mit der Durchführung oder Dauer einer Störungsbehebung nicht einverstanden sein, besteht die Möglichkeit der Eskalation über die zuständige IT-Stelle des Kunden.

4.15.3 Ticket Dokumentation in Remedy

Die Dokumentation im Tool (Remedy) und die Weiterleitung und Kommunikation über den UHD gelten sowohl für die Dataport internen Supportgruppen als auch für den Support, der durch Kunden selbst geleistet wird (z.B. fachliche Leitstellen der Kunden oder Gruppen zur fachliche Betreuung für Verfahren). Bei der Anbindung der Fachliche Betreuungsgruppen für Verfahren muss mit den Supportmitarbeitern beim Kunden ein entsprechendes Vorgehen vereinbart werden und es muss sichergestellt werden, dass die am Incident Management Prozess beteiligten Supportmitarbeiter im gleichen Tool (Remedy Web Client) arbeiten.

4.15.4 Reaktionszeiten

Reaktionszeit		
Kennzahl		Leistungsausprägung
Reaktionszeit bei Störungen (während der Servicezeit)	Priorität Kritisch (1)	0,5 Stunden
	Priorität Hoch (2)	1 Stunde
	Priorität Mittel (3)	2 Stunden
	Priorität Niedrig (4)	4 Stunden

4.15.5 1st Level UHD Dataport

Annahme und Protokollierung der Störung im Remedy, einfache Störungslösung.
Insbesondere:

- Annahme, Dokumentation und Priorisierung von Störungsmeldungen für BASIS-Anwender
- Sofortige Vermittlung von Lösungsansätzen anhand von Standard-Prozeduren und -Lösungen
- Bei Bedarf Weiterleitung von Störungen an nachgeordnete Supportinstanzen
- Fortschreiben der Lösungsdatenbank (Knowledgebase)
- Hilfestellung für Office Probleme (bis 10 Minuten)

Details → Leistungsbeschreibung User Help Desk



Die so genannte erste Unterstützung oder der Erstlösungsversuch im First Level Support erfolgt im UHD. Bei besonderer vertraglich vereinbarter Leistung kann der First Level Support darüber hinaus von einer entsprechend definierten Supportgruppe vorgenommen werden. Zunächst wird im First Level Support versucht, dem Anwender mit einem Workaround (z.B. Nutzung eines anderen Gerätes) zu helfen. Ein Workaround ist die Beseitigung durch die Bereitstellung einer schnellen bzw. zeitlich begrenzten Umgehungslösung. Der Supportmitarbeiter setzt ggf. die gemeldete Störung mit den Umgehungslösungen für bekannte Fehler und Probleme aus der Lösungsdatenbank in Verbindung.

4.15.6 2nd Level: Benutzerunterstützung BASIS

Weitergehende Problemanalyse, systemtechnische Supportaufgaben für stationäre und mobile BASIS-Kundensysteme.

- Lösung von Client Problemen
- Keine weiteren Hilfestellungen

Die Mitarbeiter im 2nd Level Support werden tätig, nachdem sie über das Tool ein Ticket erhalten haben, in dem der Incident sowie eventuell bereits durchgeführte Maßnahmen beschrieben sind. Sie untersuchen und diagnostizieren den Incident und dokumentieren zeitnah die Bearbeitungsschritte zur Lösung in dem Ticket. Hierzu gehört die Bewertung der Störungsdetails, die Erfassung und Analyse der zugehörigen Informationen sowie Lösungen und die Prüfung von Störungsmustern. Der Fachbereich setzt den Incident auf „gelöst“ und somit ist die Störung behoben. Die Anwenderin oder der Anwender erhält aus dem Ticket heraus eine standardisierte Meldung über die Lösung der Störung.

4.15.7 2nd/ 3rd Level: Sharepoint Competence Center – Betrieb

Lösung von Problemen der SharePoint Infrastruktur, ggf. weiterleiten von Problemen an den Produkthersteller Microsoft.

- Lösung von Infrastruktur Problemen (Server Probleme)
- Keine weiteren Hilfestellungen
- Ggf. Unterstützung durch SharePoint Berater sofern durch Fachliche Leitstelle SharePoint abgedeckt

4.16 Changemanagement

Veränderungen an den Infrastrukturdiensten können aus folgenden Ursachen notwendig werden:

- Modernisierung aufgrund der technischen Weiterentwicklung;
- Ersatz von Systemen im Rahmen der Erhaltung der Infrastruktur und der Dienste; die Abstimmung erfolgt mit den betroffenen Kunden



- Veränderung oder Erweiterungen der Infrastrukturdienste aufgrund von Kundenaufträgen; Art und Umfang sind hier durch den Auftrag bestimmt

Changes mit Auswirkungen auf die Verfügbarkeit der Infrastrukturdienste erfolgen im Wartungsfenster oder zu gesondert abgestimmten Terminen. Die Termine werden von einem Gremium der Fachlichen und Technischen Leitstelle SharePoint abgestimmt.

4.16.1 Changes mit Zustimmung bei Vertragsabschluss

Veränderungen, die zur Behebung einer Störung mit großflächiger Auswirkung oder zur Abwendung eines akut anstehenden Systemausfalls unabwendbar sind, werden als „Emergency-Change“ ohne vorherige Zustimmung im Einzelfall durchgeführt.

Anforderungen zur Leistungserhöhung sind unter Einhaltung einer angemessenen Vorlaufzeit möglich. Die entsprechenden Aufwände werden gesondert in Rechnung gestellt. Ebenso erhöhen sich die laufenden Leistungsvergütungen.

Änderungen an der technischen Infrastruktur durch den Auftragnehmer zum Zweck der Erhaltung, der Erneuerung oder der Erweiterung, werden den betroffenen Kunden mindestens 7 Tage vorher angekündigt.

Changes, welche der normalen Betriebsführung dienen, wie Security-Patches, HW-Tausch etc. bedürfen keiner gesonderten Genehmigung durch den Auftraggeber.

4.16.2 Changes mit Zustimmung im Einzelfall

Changes, die zu Änderungen der mit dem Auftraggeber abgestimmten Architektur führen oder zu erheblichen Aufwandssteigerungen beim Auftragnehmer führen, sind vom Auftraggeber freizugeben.

Für die Realisierung individueller Wünsche der Kunden wird der Auftragnehmer ein Angebot auf der Grundlage der vom Auftragsberechtigten definierten Anforderungen abgeben.

4.17 SharePoint Designer

Der Einsatz von SharePoint Designer ist auf der produktiven Infrastruktur nicht zugelassen. Der Einsatz des SharePoint Designers ist ausschließlich in der Entwicklungsumgebung erlaubt. Mit SharePoint Designer erstellte Lösungen können gemäß Regelwerk („Deployment von Kundenlösungen“) auf der Produktivumgebung installiert werden. Die Übertragung von SharePoint Designer Änderungen, wie selbst erstellten Workflows ist nur eingeschränkt möglich.

4.18 Deployment und Betrieb von (Kunden)Lösungen

Alle Kundenlösungen müssen den Regeln des AN für Eigenentwicklungen und Drittanbieterlösungen nachkommen, um auf der zentralen Infrastruktur betrieben zu werden. Eine Orientierungshilfe geben dieser Abschnitt und der „Development Guide“.

Werden diese Regeln nicht eingehalten ist ein Betrieb nicht möglich.

Die SharePoint Server Farm in der zentralen Infrastruktur wird mit geringen Anpassungen betrieben, es wird ein hoher Standardisierungsgrad und größtmögliche Betriebssicherheit angestrebt.

4.18.1 Allgemeine Regeln und Grundsätze

In der SharePoint Server Farm gelten folgende Regeln und Grundsätze, um eine sicheren und kostengünstigen Betrieb zu gewährleisten:

- Höchste Priorität haben Update-Fähigkeit, Betriebssicherheit und Vermeidung von Spezial-Entwicklung („Sonderlocken“).
- Beratung, Architektur und Entwicklung sind am Betrieb der Infrastruktur orientiert.
- Für die gleichen fachlichen Anforderungen gibt es jeweils nur eine Lösung, Mehrfachentwicklungen sind zu vermeiden.
- Lösungserstellung ohne Code unter Benutzung von SharePoint Standard Funktionalität für dafür geeignete Anforderungen hat oberste Priorität.
- Erweiterung der Standardmöglichkeiten durch Entwicklung von wieder verwendbaren Komponenten für eine möglichst große Kundengruppe hat die nächst höhere Priorität. Grundlage für die Entwicklung sollen nach Möglichkeit Standardfunktionalitäten sein.
- Eigenentwicklungen für Anforderungen, die nicht durch den Standard abgedeckt sind (Fachanwendungen) werden nur nach Genehmigung durch das SharePoint Competence Center und die Fachlichen Leitstellen zugelassen. Die Freigabe wird dokumentiert.
- Der AG formuliert fachliche Anforderungen, keine Umsetzungsanweisungen. Das SCC erarbeitet gemeinsam mit dem AG daraus die entsprechende Lösung und Implementierung.

4.18.2 Klassifizierung von Anpassungen

Microsoft SharePoint Server ist ein sehr flexibles Werkzeug für die Erfassung, Bearbeitung, Ablage und das Wiederfinden von Informationen. Trotz der vielen Möglichkeiten, die eine Standardinstallation bietet, ergeben sich im täglichen Arbeitsleben besondere Anforderungen, für die Anpassungen erforderlich sind.

Die Anpassungen können entsprechend der Berechtigungen eines Benutzers oder dem Zugriff auf bestimmte Komponenten in verschiedene Klassen eingeordnet werden:

4.18.2.1 Erstellung und Anpassung von Inhalten

Kann von Benutzern mit Teilnehmer-Rechten im SharePoint über den Browser vorgenommen werden.



- Webparts personalisieren (Hinweis: wird nur von einigen Webparts unterstützt)
- Erstellung, Anpassung von Inhalt und Layout und Löschung von Veröffentlichungsseiten (z.B. Artikeln, Nachrichten).

4.18.2.2 Einfache Anpassungen an Layout und Struktur

Kann von Benutzern mit Designer-Rechten über den Browser vorgenommen werden.

- Listen und Bibliotheken erstellen, konfigurieren und löschen
- Öffentliche Ansichten in Listen und Bibliotheken erstellen, ändern und löschen
- Seiten erstellen, bearbeiten und löschen
- Webparts auf einer Seite platzieren, konfigurieren und löschen
- Liste oder Bibliothek als Vorlage speichern
- Website als Vorlage speichern (Hinweis: diese Funktion steht nur auf Zusammenarbeitsseiten/Teamsites zur Verfügung)
- Lokale Inhaltstypen, die auf Standardinhaltstypen und Standardfeldtypen beruhen
- InfoPath-Formulare ohne oder mit skriptbasierter Logik

4.18.2.3 Einfache Anpassungen an Design und Funktion

Kann vom Websitesammlungsadministrator über den Browser vorgenommen werden.

- Microsoft Office Integration verwalten
- Kopfgrafik austauschen
- Farbgebung anpassen

4.18.2.4 Lokale Funktionserweiterungen (Sandboxed Solutions)

Genehmigung durch Fachliche Leitstelle, Deployment und Freigabe durch die technische Leitstelle.

- Webparts mit lokalem Anwendungsbereich
- Logikkomponenten, die die clientseitig verfügbaren Anwendungsschnittstellen oder die geschützte serverseitige Anwendungsschnittstelle verwenden
- Lokale Listen- und Bibliotheksvorlagen
- Lokale Inhaltstypen
- Lokale Websitespalten

4.18.2.5 Globale Funktionserweiterungen (Farm Solutions)

Genehmigung durch Fachlichen Leitstelle(n), Deployment und Freigabe durch die technische Leitstelle. Die technische Leitstelle entscheidet, welche fachlichen Leitstellen eingebunden werden müssen.

- Globale Designanpassungen, die den grundlegenden Seitenaufbau (Masterpage / PageLayouts), die angebotenen Farben, Schriftarten sowie Format- und Markupvorlagen umfassen.
- Austausch des Favoriten-Icons
- Webparts mit globalem Anwendungsbereich oder erhöhtem Sicherheitskontext zur Laufzeit
- Globale Inhaltstypen (z.B. für das Intranet)
- Globale Feldtypen (z.B. Ampelfeld)
- Seitenvorlagen (z.B. „Artikel (Bild rechts oben)“)
- Websitevorlagen / Websiterezepte (z.B. Nachrichtencenter)
- Globale Erweiterungen von Menüs und Kontextmenüs
- Bereitstellung von Dialogfenstern (z.B. Portalnavigator)
- Logikkomponenten, die auf die vollständige Serverschnittstellen oder eine Ausführung im erhöhten Rechtekontext angewiesen sind
- Bereitstellung von Anwendungsbibliotheken im Global Assembly Cache
- Modifikation der Webanwendungskonfiguration (web.config)
- Dokumentensymbole anpassen
- Website-, Listen-, Bibliotheks- oder Elementaktionen (Event Receiver, Custom Actions und Event Handler)
- Zeitgeberaufträge (TimerJobs, z.B. LinkChecker)
- Webservices, die von anderen Komponenten konsumiert werden können
- Anwendungsseiten („_layouts“-Seiten)
- Workflows und Workflow-Aktivitäten
- InfoPath-Formulare mit Programmlogik

4.18.2.6 Nicht erlaubte Anpassungen

- Modifikation von SharePoint Systemdateien
- Websitesammlungsdefinitionen bzw. Websitedefinitionen (SiteDefinitions bzw. SiteTemplates); Websitevorlagen (Web Templates: *.wsp-Dateien) und Websiterezepte (Site Recipes: *.xml-Dateien) sind hingegen erlaubt.
- Windows Dienste
- http-Handler bzw. http-Module
- Zugriff auf SharePoint Datenbanken (Ausnahme: Logging-DB, die jedoch Stand April 2011 nicht in Betrieb ist)

4.18.3 Lösungsentwicklung



Es gibt folgende Möglichkeiten der Lösungsentwicklung.

4.18.3.1 Entwicklung durch/mit SharePoint Competence Center

Die Entwicklung erfolgt durch das SharePoint Competence Center von Dataport oder unter Begleitung durch das SCC.

4.18.3.2 Eigenentwicklungen durch AG

AG entwickelt selbst oder beauftragt die Entwicklung bei einem Fremdanbieter, der AG hat Zugriff auf den Quellcode. Die Entwicklung ist mit technischer und fachlicher Leitstelle abgestimmt und genehmigt.

4.18.3.3 Drittanbieterlösungen

Drittanbieterlösungen werden auf der Standard Infrastruktur nur nach Freigabe durch die Fachlichen Leitstellen SharePoint und die technische Leitstelle verwendet. Die Freigabe wird dokumentiert.

Die Entscheidungsfindung erfolgt anhand des aus gefüllten Formulars:

- „Anlage 4 SharePoint Betrieb Dokumentation Drittanbieterlösungen“

Für komplexe Anwendungen mit hohem Anpassungsgrad von Drittherstellern werden separate Infrastrukturen betrieben.

Die Aufwände für den Betrieb einer eigenen Infrastruktur für Drittanbieterlösungen sind nicht Bestandteil der allgemeinen Betriebskosten und werden gesondert berechnet. Der AN kann keinen Support für Drittanbieterlösungen garantieren.

4.18.4 Regeln für Lösungsentwicklung

Um die Entwicklung und Implementation von Anwendungen zu strukturieren und zu vereinheitlichen, ist ein Regelwerk für Eigenentwicklungen definiert. Ziel ist es, die Standardisierung der Anwendungsentwicklung und der dazugehörigen Dokumentation zu gewährleisten.

Die Übergabe der Lösung erfolgt über eine spezielle SharePoint-Site, die sogenannte **Anwendungsdatenbank**. Diese ist für jede Lösung vollständig auszufüllen (Anwendungssteckbrief, Dokumentation, Testfälle, WSP, etc.).

4.18.4.1 Anwendungsdatenbank

Zentraler Ablageort für sämtliche Entwicklungen ist die Anwendungsdatenbank:
<http://betrieb.scc.intranet.dataport.de/AnwDB/Seiten/default.aspx>.

Für die jeweiligen Anwendungen werden hier eigene Arbeitsbereiche erstellt, sie umfassen Ablageorte für die Solutions / Software, Dokumentation und Testfälle. Für die Zusammenarbeit der einzelnen Personen stehen Ankündigungen, Anforderungslisten, Fehlerlisten und eine Terminübersicht zur Verfügung.

Auf die Anwendungsdatenbank haben die Betreiber, Entwickler und Kunden/Projektmitglieder gleichermaßen Zugriff.

In der Regel haben die Entwickler direkt Zugriff auf die Anwendungsdatenbank. Sie stellen selbständig die Software in der entsprechenden Bibliothek bereit und pflegen die dazugehörigen Metadaten. Im Ausnahmefall kann die Software an das Postfach web-services@dataport.de geschickt werden. Das Einstellen der Software in die Anwendungsdatenbank und die Pflege der Metadaten wird dann vom Betrieb vorgenommen.

Hinweis:

Softwareauslieferungen an die personalisierten Email-Adressen des Betriebes sind nicht erwünscht und gelten als nicht ausgeliefert. Auch sollte es unterlassen werden mit der Email an das Postfach web-services@dataport.de Betreiber mit in cc zu adressieren.

4.18.4.2 Checkliste für Entwicklungen

Die Checkliste für Entwicklungen wird vom AG eingehalten:

- Einhalten der Regeln im „Development Guide“.
- Einhalten des Entwicklungsprozesses mit Checkpoints, Übernahme der Kosten von Checkpoints und Tests für Eigenentwicklungen und Drittanbieterlösungen
 - Architektur und Design Review
 - Code Review
 - Review Dokumentation und Testfälle
 - Review Testplan/ Testpläne
- Pflege der Anwendungsdatenbank im SCC Portal, insbesondere
 - Erstellen eines Anwendungssteckbriefes
 - WSP-Datei(en): Lösung (wsp) wird nur über die Anwendungsdatenbank an den Betrieb geliefert
 - Power Shell Installationsskript
 - Angabe der Zielinfrastruktur

- Angabe, ob Sandbox- oder Farm-Solution (mit Begründung)
- Vollständige Dokumentation sowohl in Form von Dokumenten in dem Dokumentationsbereich der Anwendung als auch in Form von Ankündigungen liegt vor
 - Betriebsdokumentation
 - Benutzerdokumentation
- Testfälle und Testpläne/-protokolle werden zur Verfügung gestellt
- Pflege und Nutzung der Fehlerdatenbank in der entsprechenden Anwendung
- Automatisierte Codeüberprüfung ergibt keine Fehler bzw. Fehler sind verstanden und unkritisch
 - Dispose Checker: Suche nach Memory Leaks
- Für Drittanbieterlösungen: „Anlage 4 SharePoint Betrieb Dokumentation Drittanbieterlösungen“ wird zur Verfügung gestellt
- Wurde die Software von einem Drittanbieter entwickelt und erfolgt mit der Übergabe in den Betrieb auch eine Übergabe der Wartungsaufgaben an Dataport, sind folgende Bestandteile zusätzlich zu übergeben:
 - Quellcode
 - Entwickler-Dokumentation
- Für FHH/BASIS-Kunden: Soll der User Help Desk von Dataport Supportleistungen übernehmen, so muß folgende Dokumentation zur Verfügung gestellt werden:
 - Support_Informationen mit typischen Problemen und Lösungswegen in der Anwendungsdatenbank und per E-Mail an das Funktionspostfach DataportUHD@Dataport.de.
Die Support-Information wird vom UHD in ein Knowledgebase-Artikel umgewandelt.

Freigabe der Lösung von Fachliche(n) Leitstelle(n) und technischer Leitstelle vor Deployment auf Stage und Produktivumgebung ist erforderlich. Der SharePoint Deployment Prozess muss eingehalten werden.

4.18.4.3 Übergabe der Lösung

Jede Software muss vor dem Deployment vorher in der Anwendungsdatenbank eingepflegt werden.

Zum Einpflegen gehört:

- Speicherung der Software, in der Regel WSP-Dateien, gezippt ohne Passwort.
Der Dateiname der ZIP-Datei besteht aus dem Namen der Lösung und der aktuellen Versionsnummer (Beispiel: FHHportal.Branding.Solutions.REL.1.2.zip)
- Metadaten in der Softwarebibliothek:
 - Das Metadatum „Kurzbeschreibung“ dokumentiert die Veränderungen zur Vorversion bzw. gibt nähere Details zur Version an.
 - Das Metadatum „Status“ dient der Übersicht, in welcher Umgebung welche Version aktuell deployed ist. Beim Hochladen wird dies standardmäßig auf „undeployed“ gesetzt. Das Feld wird nur vom Betrieb nach Installationen verändert.
 - Alle weiteren Metadatenfelder sollten nach bestem Ermessen gefüllt werden, um die Solution mit Infos anzureichern.
 - Bei ausführlichen Veränderungen/Beschreibungen bitte auf die Doku verweisen, anstatt ein Metadatenfeld zu überfüllen, z.B. bei Abhängigkeiten: „s. Doku“ eintragen

4.18.4.4 Fristen für die Unterstützung neuer SharePoint Versionsstände

Für die Fristen bezüglich der Unterstützung von Updates und neuen SharePoint-Versionen gelten folgende Verpflichtungen für den Auftraggeber:

- SharePoint Versionen 6-12 Monate nach Ankündigung durch Microsoft zu unterstützen
- SharePoint Servicepacks 1 Monat nach Ankündigung durch Microsoft zu unterstützen
- Alle SharePoint / Betriebssystem Hotfixes sofort zu unterstützen

Werden die Fristen nicht eingehalten, kann die Anwendung nicht mehr in der zentralen Infrastruktur betrieben werden. Ggf. müssen Anwendungen, auf die dies zutrifft, in eigenen SharePoint Farmen betrieben werden.

4.18.4.5 Organisatorische Regeln

Benennung einer Entwicklungsleiters / Koordinators als Ansprechpartner für den AN.

Kosten für ressourcenintensiven (Hardware und/oder Personal) Betrieb werden übernommen.

4.18.5 Paketierung und Installation

4.18.5.1 Solution (WSP)

SharePoint-Lösungen müssen zwingend als **WSP** ausgeliefert werden. Weder direkte Kopieroperationen auf den Servern der Farm noch die Installation von Features ohne eine Kapselung in eine Solution sind zulässig. Allein über Solutions ist eine automatische Synchronisation der Server sowie eine vollständige Deinstallation erreichbar.

4.18.5.2 GAC- bzw. bin-Installation von Assemblies

Assemblies werden je nach Anforderung der Erweiterung im GAC oder im bin-Ordner installiert.

4.18.5.3 Installation von Dateien im SharePoint-Root

Dateien, die in den SharePoint-Root-Ordner deployed werden, müssen in den vorgesehenen Standard-Ordner abgelegt werden (z. B. CONTROLTEMPLATES, IMAGES, etc.). Unterhalb dieser Ordner muss immer ein lösungsspezifischer Unterordner angelegt werden.

4.18.5.4 Installationsskripte

Die Installation von Lösungen muss komplett automatisiert via Power Shell-Skript erfolgen („One Click Deployment“). Manuelle Schritte dürfen nur in begründeten Ausnahmen erforderlich sein. Für die Erstellung der Skripte stellt Dataport eine Power Shell-Methodensammlung bereit (Dataport.SharePoint.Powershell.CommonDeploy.ps1).

Pro Solution sind folgende Skripte zu erstellen:

- Install/Update
- Uninstall

Besteht eine Lösung aus mehreren Solutions ist für Install, Uninstall und Update auch jeweils ein Masterskript bereitzustellen, das die einzelnen Skripte der Solutions aufruft.

Sind für unterschiedliche Umgebungen unterschiedliche Installationsparameter erforderlich (z. B. URLs), so ist jeweils ein Skript pro Umgebung zu erstellen.

4.18.5.5 Upgrade und Löschen von Erweiterungen

Besondere Vorsicht ist bei einem Upgrade oder dem Löschen vorhandener Erweiterungen geboten. Es ist im Vorfeld zu prüfen, welche Auswirkungen die Aktion auf vorhandene Instanzen, die auf der Erweiterung aufsetzen, hat. Eventuelle Gegenmaßnahmen (Feature-Versionierung und –Upgrade, Assemblyversionierung, Binding Redirects, Erstellung eines Neuen Features/Verstecken des alten Features, etc.) sind bereits in der Entwicklung zu berücksichtigen.



4.18.6 Deployment und Freigabeprozess

Dieser Abschnitt beschreibt den Deploymentprozess für die von Dataport betriebenen SharePoint-Umgebungen (Integration-, Stage- und Produktionsumgebung). Der beschriebene Prozess ist bindend für das Deployment von Neuentwicklungen von Solutions / Features, das Einbinden von InfoPath-Formularen sowie vergleichbare Anpassungen der Sharepoint Infrastruktur.

In der Regel besteht der Deploymentprozess in der Bereitstellung einer Solution durch die jeweiligen Entwickler, sollten jedoch Lösungen nur in einer anderen Form bereitgestellt werden können, ist der gleiche Prozessablauf zu verfolgen.

Ein Deployment muss über einen festgelegten **Freigabeprozess** (InfoPath-Formular) explizit genehmigt werden. Das Deployment erfolgt über das Integrations-System und Stage-System nach entsprechenden Tests und Freigaben in die Produktion.

4.18.6.1 Beauftragung

Das Deployment, in welchem System auch immer, muss beauftragt werden. Dazu wird ein Infopath-Formular mit hinterlegtem Genehmigungsworkflow in der Anwendungsdatenbank bereitgestellt. In diesem Formular werden folgende Angaben zum Ausführen des Auftrages abgefragt:

- Auswahl der Anwendung
- Geplanter Termin
- Selektion der Pakete mit dem jeweiligen Auftrag (Update/Install/Reinstall/Deinstall)
- Weitere Hinweise für den Betrieb

Alle weiteren Daten werden aus den Metadaten der Anwendung entnommen. Die Hinweise für den Betrieb sind zwingend auszufüllen und möglichst detailliert zu beschreiben (TimerJob Resets, anschließende Konfigurationen, Aktivierung von Features, etc). Dies soll die Funktionalität der Lösung nach dem Deployment sicherstellen. Sofern keine Konfiguration, etc. im Anschluss erforderlich ist, so ist dies ebenfalls explizit zu nennen.

Nach Antragstellung startet der Workflow und holt entsprechende Genehmigungen der beteiligten Leitstellen und Verantwortlichen ein. Die Zuständigen können je nach Anwendung und Deployment-status (Integration/Stage/Produktion) differieren und werden aus den Metadaten der Anwendung ausgelesen. Per E-Mail werden die entsprechenden Zuständigen über die Aufgaben informiert. Bei Annahme/Ablehnung des Antrags erhalten die Leitstellen und der Entwickler entsprechend sofort Feedback.

Das Formular ist für den vollständigen Ablauf des Prozesses konzipiert. Es ist nicht möglich eine Farm zu überspringen oder die Fristen zu unterschreiten (s. 5.18.7.4). Das Formular speichert den aktuellen Status und wird somit für die Aktualisierung aller Farmen fortlaufend genutzt.



4.18.7 Termine und Betriebszeiten für Deployments

4.18.7.1 Produktion

Die Installation von Solutions oder Features, das Einbinden von InfoPath-Formularen sowie vergleichbare Anpassungen in der Produktion erfolgt jeweils am zweiten Dienstag im Monat ab 19:00 Uhr. Softwareupdates erfolgen aufgrund der Installationsdauer an im Einzelfall zu vereinbarenden Wochenenden.

Das Deployment in die Produktion muss bis Freitag Dienstschluss mit allen o.a. Unterlagen beauftragt sein, damit der Change durchgeführt werden kann.

4.18.7.2 Stage

In der Stage findet ein wöchentliches Deployment am Dienstag statt. Das Deployment muss ebenfalls bis Freitag Dienstschluss mit allen o.a. Unterlagen beauftragt sein, ansonsten verschiebt sich die Installation auf das nächste Wartungsfenster. Am Montag bis 14 Uhr erfolgt durch den Betrieb die Prüfung der Testprotokolle mit anschließendem Feedback an den Entwickler.

4.18.7.3 Integration

In der Integrationsumgebung findet ein wöchentliches Deployment am Donnerstag statt. Das Deployment muss bis Dienstag Dienstschluss mit allen o.a. Unterlagen beauftragt sein, ansonsten verschiebt sich die Installation auf das nächste Wartungsfenster. Am Mittwoch bis 14 Uhr erfolgt durch den Betrieb die Prüfung der Solution und der Dokumentation mit anschließendem Feedback an den Entwickler.

4.18.7.4 Generelles

Sollen an einem Deploymenttermin mehr als 2 Updatepakete (bestehend aus mehreren Solutions, z.B. HIM-Workflow, Dataport Internetauftritt) oder mehr als 5 Einzelsolutions bereitgestellt werden, so behält sich der Betrieb vor einzelne Pakete in Absprache mit dem Kunden auf das nächste Wartungsfenster zu verschieben. Mit diesem Vorgehen sollen schnellere Analysen im Fehlerfall gewährleistet werden können.

Die Fristen und Testphasen ergeben sich nach dem obigen Deploymentprozess wie folgt:

3 Wochen vor Installationstermin in der Produktion ist der letzten Termin zur Beauftragung von Anpassungen, die zunächst am Donnerstag wie oben beschrieben in der Integrationsumgebung erfolgen. Diese müssen zunächst in dieser getestet werden, das resultierende Testprotokoll wird dann für das folgende Deployment in der Stage angefügt. Es stehen somit 6-7 Werkzeuge fürs Testen in der Integration zur Verfügung. 1,5 Wochen später darf frühestens der Antrag für die Stage gestellt werden. Hier erfolgt ein 3-4 Werkzeuge langer Test bevor der Antrag für die Produktion erfolgen darf.



Es wird keine Beauftragung ohne die Einhaltung der Voraussetzungen akzeptiert. Ansonsten gilt das nächste Wartungsfenster.

4.18.8 Sandboxed Solutions

Site Collection Administratoren wird nicht das Recht gewährt, Sandboxed Solutions zu installieren. Das Deployment erfolgt stattdessen, analog zu Farm Solutions, über den Betrieb.

Für den Einsatz von Sandboxed Solutions muss eine Begründung vorliegen. Standardmäßig sind die Sandboxed Solutions deaktiviert.

4.19 Unterstützung bei Fragen zur Sicherheitskonzept, Datenschutz und Berechtigungen

Sofern der AG im Zuge von Dienstvereinbarungen, Datenschutzregelungen oder aus anderem Anlass Unterstützung im Bereich SharePoint Administration benötigt, wird diese durch den AN gewährt und muss separat beauftragt werden. Fachlich umfasst diese Unterstützung die Bereiche Datenschutz und Berechtigungen, sofern sich die Themen auf die Grundfunktionen des SharePoint Servers beschränken.

Fragen, die sich durch fachliche Anforderungen in konkreten Projekten ergeben, sind von der Unterstützung nicht betroffen. Der AN unterstützt z.B. bei der Schilderung der Standardberechtigungen im SharePoint. Eine konkrete Umsetzung von Berechtigungsstrukturen ist jedoch Teil der Fachkonzeption und muss vom AG geliefert werden. Eine separate Beauftragung von Berechtigungs- und Sicherheitskonzept ist möglich. Hierfür muss ein eigenes Angebot erstellt werden.

Generell obliegt die Farmadministration ausschließlich dem AN, die Vergabe und Pflege der Berechtigungen innerhalb der Websitesammlungen werden vom AG übernommen.



5 Servicezeiten und Support

Leistung	
Betriebszeiten: - betreuter Betrieb - überwachter Betrieb	Mo. – Do.: 08.00 – 17.00 Uhr Fr.: 08.00 – 15.00 Uhr Übrige Zeit: Bedienerlose Online Verfügbarkeit
Servicezeit:	Mo. – Do.: 08.00 – 17.00 Uhr Fr.: 08.00 – 15.00 Uhr

Der AN ist in der Servicezeit über ein Auftragspostfach (Web-Services@dataport.de) oder unter der Rufnummer 040-428 46 1952 erreichbar.

Der AN wird Störungen seiner technischen Einrichtungen im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten innerhalb der Regelentstörzeit beseitigen (montags bis donnerstags von 08.00 bis 17.00 Uhr und freitags von 08.00 bis 15.00 Uhr, soweit diese Tage keine gesetzlichen Feiertage sind). Mit der Entstörung wird unverzüglich, spätestens jedoch innerhalb von 4 Stunden nach Eingang der Störungsmeldung begonnen.



6 Mitwirkung des Auftraggebers

6.1 Webanwendungsadministratoren

Der AG benennt 2 Benutzer als Webanwendungsadministratoren (ggf. eine Fachliche Leitstelle). Diese Benutzer erstellen das Sicherheitskonzept und treffen grundlegende Entscheidungen über den Aufbau der Webanwendung.

Dazu gehören

- Entscheidungen über die Anlage von Websitesammlungen
- Entscheidungen über das Design
- Entscheidungen über die Einrichtung eines MySite-Hosts
- Entscheidungen über die Nutzung von Web-Services
- Entscheidung über Zugriffsszenarien z.B. über UAG

6.2 Websitesammlungsadministratoren

Der AG benennt -2- Benutzer als Eigentümer, diese sind die Websitesammlungsadministratoren. Diese Benutzer verwalten die Inhalte, Strukturen und Berechtigungen und sind die einzigen Kontaktpersonen seitens des AGs zum AN.

6.3 Schutzbedarfeinstufung

Der AG legt dem AN schriftlich eine Schutzbedarfseinstufung seiner geplanten Ablagedaten nach BSI-Grundschutz bzw. gemäß der für ihn gültigen Datenschutzvorschriften vor. Der AG ist für eine regelmäßige Überwachung der Einstufung des Schutzbedarfes seiner Daten selbst verantwortlich. Bei einer Änderung der Einstufung ist dieses dem AN umgehend mitzuteilen. Im Falle der Änderung dieser Einstufung muss ggf. erneut über den Vertrag verhandelt werden.

7 Anhang

7.1 Dokumentation

- Development Guide, auch als Anlage zum Vertrag:
 - <http://scc.intranet.dataport.de/Rahmenvertrage/DevelopmentGuideSP2010.pdf>
- Service Level Agreement -Infrastrukturdienste im FHHNet:
 - <http://fhhportal.stadt.hamburg.de/websites/1003/za/PAG/BASIS-Newsletter/BASISSLA%20und%20begleitende%20Dokumente/Forms/AllItems.aspx>



Anlage 3 zum Vertrag V5378/2300000

SharePoint Competence Center

Entwicklung und Beratung im SharePoint Umfeld Leistungsbeschreibung

Version 1.1
Vom 21.06.2011

Inhaltsverzeichnis

1	Zusammenfassung.....	1
2	SharePoint Beratung.....	2
2.1	Durchführung von Workshops ("Getting Started") zur Einführung von SharePoint in Organisationseinheiten, Projektteams, etc.	2
2.2	Gemeinsames Erarbeiten der SharePoint-Strategie einer Behörde.....	2
3	SharePoint-Lösungsentwicklungen	3



1 Zusammenfassung

Das SharePoint Competence Center (SCC) bietet Beratungs- und Entwicklungsleistungen im Zusammenhang mit der Technologie SharePoint an. Vornehmlich handelt es sich bei diesen Dienstleistungen um Entwicklung, Beratungen, Konzeptentwicklungen und Schulungsleistungen. Das SCC ist für die Kunden zentraler Ansprechpartner für SharePoint-Lösungsentwicklung. Zusätzlich dazu stimmt sich das SCC mit den jeweiligen Fachlichen Leitstellen SharePoint regelmäßig ab, um die SharePoint Plattform kontinuierlich weiterzuentwickeln.



2 SharePoint Beratung

2.1 Durchführung von Workshops ("Getting Started") zur Einführung von SharePoint in Organisationseinheiten, Projektteams, etc.

- Einführung in die SharePoint Technologie
- Einführung in das jeweilige Portal/ Webanwendung und seine Architektur
- Ggf. Beginn der Aufnahme der Anforderungen
- Erläuterung der Möglichkeiten von SharePoint zur Lösung der Fachaufgaben der Behörden mit SharePoint Standard Funktionalität
- Erstellung eines Plans für das weitere Vorgehen
- Gegebenenfalls erste Umsetzung der Absprachen

2.2 Gemeinsames Erarbeiten der SharePoint-Strategie einer Behörde

- Aufnahme der Anforderungen
- Erarbeitung der Möglichkeiten von SharePoint zur Lösung der Fachaufgaben des Kunden mit SharePoint Standard Funktionalität
- Umsetzung der Absprachen



3 SharePoint-Lösungsentwicklungen

Wenn sich Anforderungen nicht mit der Standard-Funktionalität unter SharePoint umsetzen lassen, kann der Funktionsumfang durch Individualentwicklung entsprechend erweitert werden. Für solche Erweiterungen bieten wir sämtliche Dienstleistungen entlang des Software-Lebenszyklus' an, insbesondere:

- **Planung/Analyse:** Aufnahme und Dokumentation der Kundenanforderungen an eine Sharepoint Lösung
- **Entwurf:** Prüfung und Vorgabe des Lösungswegs und einer Architektur zur Erfüllung der Kundenanforderungen, vorzugsweise mit SharePoint Standard Funktionalität
- **Implementierung:** Umsetzung der Lösung gemäß fachlichen und technischen Vorgaben
- **Test:** Sicherstellung qualitativ hochwertiger Lösungen durch automatisierte und manuelle Tests
- **Dokumentation:** Erstellung von Betriebs-, Anwender- und Entwicklerdokumentation
- **Deployment:** Übergabe der Lösung an den Betrieb und Abwicklung des Deploymentprozesses
- **Wartung:** Erweiterung vorhandener Lösungen auf Basis neuer Kundenanforderungen



Anlage 4 zum Vertrag V5378/2300000

SharePoint Competence Center

Dokumentation Drittanbieterlösungen Formular

Version 1.1
Vom 23.06.2011

Inhaltsverzeichnis

1	Einführung	1
2	Release-Freigabeformular.....	1
2.1	Grundlegende Maßnahmen.....	1
2.2	Abkürzungen	1
2.3	Änderungen.....	2
2.4	Geschäftsvorfall und Deployment-Datum	2
2.5	Design-Übersicht.....	2
2.5.1	Logische Architektur	2
2.5.2	Physikalische Architektur.....	2
2.6	Detailliertes Design	2
2.6.1	Elemente einer Site	2
2.6.2	Kapazitätsplanung	3
2.7	Kundenspezifische Datenbanken	3
2.8	Exception Handling	3
2.9	Sicherheit	3
2.10	Produkte von Drittanbietern	3
2.11	Web Services	3
2.12	SharePoint Konfigurationseinstellungen	4
2.13	Deployment.....	4
2.14	Verschiedenes.....	4
2.15	Annahmen.....	4
2.16	Liste der benötigten Dokumente.....	4
2.17	Referenzen.....	5



1 Einführung

Das SharePoint Competence Center (SCC) als zentraler Ansprechpartner für Kunden im Bereich SharePoint ist verantwortlich für den stabilen Betrieb der SharePoint-Landschaft. Ziel ist es, den Kunden eine stabile und performante SharePoint-Umgebung zur Verfügung zu stellen. Daraus resultierend müssen Änderungen am System wie z.B. die Installation von SharePoint-Erweiterungen einen Prozess durchlaufen und bestimmten Qualitätsanforderungen genügen. In diesem Dokument wird ein Formular (Release-Freigabeformular) bereitgestellt, welches auszufüllen ist, bevor eine Anwendung eines Fremdherstellers durch das SCC zur Verfügung gestellt wird. Unter einem Release wird dabei die Version einer Erweiterung verstanden, die ein Kunde in der SharePoint-Farm verwenden möchte.

2 Release-Freigabeformular

2.1 Grundlegende Maßnahmen

Ein Release darf nicht dazu führen, dass Anwender in ihrer Arbeit beeinträchtigt werden. Es muss begründet werden, warum Anforderungen nicht mit SharePoint-Standard-Funktionen umgesetzt werden, da die Verwendung von Standard-Funktionen mehr Sicherheit garantiert als kundenspezifische Anpassungen. Keine Anpassung darf bestehende SharePoint-Dateien überschreiben, um Probleme mit dem Microsoft-Support, Hotfixes oder Service Packs zu vermeiden. Wenn Features deinstalliert werden, muss die Deinstallation ein komplettes Rollback einleiten, es müssen alle zum Feature gehörenden Dateien und Konfigurationseinträge rückgängig gemacht werden. Es muss klargestellt werden, wie dieses gewährleistet wird. Es ist zu bestätigen, dass dieses Verhalten getestet wurde. Erfolgt diese Bestätigung nicht, wird davon ausgegangen, dass der entsprechende Test nicht erfolgt ist. Ein High Level Design-Dokument zum Release ist zur Verfügung zu stellen. Es ist darzustellen, welche Maßnahmen ergriffen worden sind, um Speicherlöcher zu vermeiden (z.B. Einsatz Dispose Checker) und Performance-Probleme zu verhindern (z.B. keine Abfragen mit sehr vielen Treffern). Es ist zu erwähnen, ob Last- oder Performance-Tests erfolgt sind (inkl. Resultate). Sofern eine Erweiterung Konfigurationsänderungen in der SharePoint-Farm oder in einer Webanwendung vornimmt, ist dies zu dokumentieren und nach Möglichkeit im Vorfeld mit dem Betrieb zu klären, um Seiteneffekte auf bestehende Applikationen auszuschließen. Konfigurationsänderungen in der web.config einer Webanwendung, welche die komplette Webanwendung betreffen, sind zu vermeiden.

2.2 Abkürzungen

Abkürzung	Bedeutung



2.3 Änderungen

Wenn das vorliegende Dokument eine Aktualisierung eines schon bestehenden, älteren Dokumentes ist, beschreiben Sie hier bitte kurz die Änderungen und verweisen auf die betroffenen Kapitel.

2.4 Geschäftsvorfall und Deployment-Datum

Bitte beschreiben die den Anlass (konkreter Geschäftsvorfall, Vorteile der Erweiterung, Kritikalität der Erweiterung aus Geschäftsperspektive) und die Anwendergruppe für die Erweiterung. Bitte geben Sie das geschätzte Deployment-Datum an. Sofern Sie eine eigene Web-Anwendung (unabhängig ob für SharePoint oder eine Eigenentwicklung) benötigen, erläutern Sie bitte den Grund.

2.5 Design-Übersicht

2.5.1 Logische Architektur

Bitte beschreiben Sie alle Anpassungen. Insbesondere sind externe Interfaces (z.B. Aufruf externer Dienste), Datenbankverbindungen und alle SharePoint-Anpassungen darzustellen.

2.5.2 Physikalische Architektur

Sofern abzusehen ist, dass für spezielle Anpassungen zusätzliche Hardware oder Änderungen an Hardware erforderlich ist (mehr SAN, zusätzliche Server), ist dieses hier zu beschreiben. Ein solcher Fall kann zum Beispiel eintreten, wenn für viele Anwender spezielle SharePoint-Services wie Excel-Services zur Verfügung gestellt werden sollen. Sollten Änderungen an der Topologie erforderlich sein, muss ein spezielles Genehmigungsverfahren durchlaufen werden, da der Aufwand nicht unerheblich ist. Bitte bedenken Sie, dass diese Maßnahmen dem Schutz der gesamten SharePoint-Farm dienen, um den Anwendern ein reibungsloses Arbeiten mit dem System zu ermöglichen.

2.6 Detailliertes Design

2.6.1 Elemente einer Site

Beschreiben Sie für die Site-Elemente Ihrer Erweiterung den Scope der Features und Abhängigkeiten zwischen verschiedenen Features. Elemente sind dabei z.B. Site Templates, List Templates, Site Content Types, Managed Paths, Work Flows, InfoPath Forms, Web Parts, Variations, Custom Java Scripts, Timer Jobs / Schedulers, Win32 API Calls/Unmanaged Code, Caching, IFilters, WCF/Web services.



2.6.2 Kapazitätsplanung

Bitte geben Sie das geschätzte Datenvolumen an, welches durch die Erweiterung voraussichtlich über einen bestimmten Zeitraum erzeugt wird (z.B. 10000 Dokumente pro Jahr mit einer geschätzten Größe von 100000 KByte). In der Regel ist diese Abschätzung schwierig, verwenden Sie im Zweifel bitte worst case-Annahmen (worst case im Hinblick auf Speicherbedarf).

2.7 Kundenspezifische Datenbanken

Sofern eine eigene kundenspezifische Datenbank erstellt wird, müssen hier das Datenbank-Schema und der Speicherbedarf angegeben werden. Benötigte Accounts, Rechte und Sicherheitseinstellungen sind aufzuführen.

2.8 Exception Handling

Der Betrieb möchte im Fehlerfalle eine schnelle Lösung finden bzw. proaktiv tätig werden können. Um das Monitoring und entsprechende Maßnahmen zu ermöglichen bzw. um Fehler schnell zu beheben, ist ein gutes Exception Handling notwendig. Bitte beschreiben Sie hier, wo Fehler bzw. kritische Ereignisse protokolliert werden. Geben Sie ggf. Event IDs und Fehlermeldungen an und wenn möglich, potentielle Ursachen. Sofern Entwicklungen anhand von Development Guidelines vorgenommen wurden, die da Thema Exception- und Error-Handling nicht beinhalten, erwähnen Sie dies bitte. Geben Sie an, wenn Error Handling nicht explizit getestet wurde.

2.9 Sicherheit

Bitte geben Sie alle benötigten Rechte und Accounts an, die für die Erweiterung benötigt werden. Für den Fall, dass ein Application Pool Account benötigt wird, ist eine ausführliche Begründung notwendig. Beschreiben Sie bitte die Maßnahmen, die getroffen wurden, ob SQL Injection, XML Injection und Cross Site Scripting-Angriffe zu vermeiden. Sofern Sie Maßnahmen gegen Injections getestet haben, erwähnen Sie dies bitte. Sollten aus Ihrer Sicht die Schutzmaßnahmen für bestimmte Anwendungen nicht nötig sein, erläutern Sie die Gründe.

2.10 Produkte von Drittanbietern

Sofern Erweiterungen von Drittanbietern installiert werden sollen, beschreiben Sie diese bitte.

2.11 Web Services

Wenn externe Web Services verwendet werden, nennen Sie bitte die benötigten Ports. Beschreiben Sie bitte kurz den Web Service.



Web Service	Port	Beschreibung

2.12 SharePoint Konfigurationseinstellungen

Bitte geben Sie alle Einstellungen für Sites, ggf. die Suche etc. an, welche Ihre Anwendung benötigt. Wenn Einträge in die web.config vorgenommen werden, ist dies besonders zu erläutern und die Änderungen hier aufzuführen. Beachten Sie, dass alle Einstellungen über Feature Receiver zu tätigen und bei der Deinstallation des Features rückgängig zu machen sind.

Änderungen in der web.config einer Webanwendung, welche die komplette Webanwendung beeinflussen, sind ohne explizite Rücksprache mit dem Betrieb und einer Genehmigung nicht erlaubt. Dies betrifft auch Änderungen, die das Debugging-Verhalten beeinflussen (Callstack=false ist nicht ändern, ebenso ist customErrors mode="On" nicht umzustellen). Nur so können Seiteneffekte auf Erweiterungen, die in den Webanwendungen gehostet werden, vermieden werden.

2.13 Deployment

Geben Sie bitte an, in welche Ordner DLLs, Features, Bilder, CSS- und Javascript-Dateien etc. installiert werden.

2.14 Verschiedenes

Bitte geben Sie hier Informationen an, die für das Verständnis der Erweiterung und deren Design hilfreich sind. Sofern Sie Risiken sehen, sind diese hier zu beschreiben. Die Nennung von Risiken hilft mit entsprechenden Risiko-minimierenden Maßnahmen, Ihren Anwendern eine stabile SharePoint-Landschaft anzubieten. Bitte schildern Sie kurz Qualitätssicherungsmaßnahmen, die während des Entwicklungsprozesses vorgenommen wurden (z.B. Code Reviews, Einsatz von Dispose Checker etc.). Sofern keine Qualitätssicherungsmaßnahmen durchgeführt wurden, erwähnen Sie dies.

2.15 Annahmen

Nennen Sie bitte alle Annahmen, die dem Design der Erweiterung zu Grunde liegen.

2.16 Liste der benötigten Dokumente

Bitte markieren Sie die Dokumente, welche für den Betrieb zur Verfügung gestellt werden:

Dokument	Vorhanden (J/N)
Installationsdokumentation	
Dokumentation für User Help Desk	



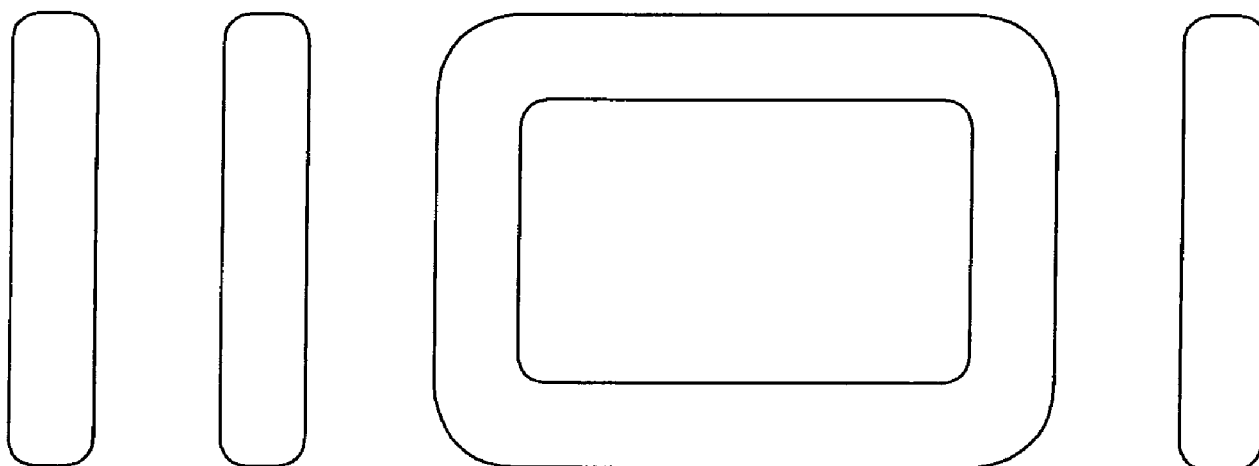
Betriebshandbuch	
Anwenderhandbuch	
Liste bekannter Fehler	

2.17 Referenzen

Sofern Referenzen existieren, welche für das Verständnis der Erweiterung hilfreich sind, geben Sie bitte hier an. Verweisen Sie bitte auf verwendete Coding Guidelines oder andere Best Practises, die verwendet wurden.

Referenz	Referenz-Link

Development- und Deployment- Guide für SharePoint



Inhalt

1	Adressaten und Zielsetzung	1
2	Überblick über den Entwicklungs- und Deployment-Prozess	1
3	Entwicklung	2
3.1	Entwicklungsumgebung	2
3.2	Entwicklungswerkzeuge	2
3.2.1	Visual Studio 2010	2
3.2.2	SharePoint Designer 2010	2
3.2.3	InfoPath 2010	3
3.2.4	Versionsverwaltung	3
3.2.5	Bug Tracking	3
3.2.6	Developer Dashboard	3
3.2.7	Weitere Werkzeuge	3
3.3	Benennung und Strukturierung von Projekten	3
3.3.1	Pfadlänge	3
3.3.2	Repository-Struktur	3
3.3.3	Ordner-Struktur in der Entwicklungsumgebung	4
3.3.4	Visual Studio Solution-Struktur	4
3.3.5	Visual Studio Project-Struktur	4
3.3.6	SharePoint Solution (WSP)-Struktur	5
3.3.7	SharePoint Feature-Struktur	5
3.4	Softwarearchitektur	6
3.5	Allgemeine Programmiervorgaben	7
3.5.1	Programmiersprache	7
3.5.2	.NET Framework-Version	7
3.5.3	Code-Konventionen	7
3.5.4	Programmierung unter SharePoint	7
3.5.5	SharePoint-Version	8
3.5.6	Customized vs Uncustomized	8
3.5.7	Interne Klassen	8
3.5.8	Fehlerbehandlung	9
3.5.9	Logging	9
3.5.10	Konfigurationsparameter	9
3.5.11	Sicherheit	10
3.5.12	Links	10
3.5.13	Interne Namen	10
3.5.14	Browserkompatibilität	10
3.5.15	Barrierefreiheit	10
3.5.16	Lokalisierung	10
3.5.17	Reservierte Query String-Parameter	10
3.5.18	Versionsverwaltung	11
3.6	Claims	11
3.6.1	Funktionseinschränkungen durch Claims	11
3.6.2	Programmiervorgaben für den Umgang mit Claims	12
3.7	Performance	14
3.7.1	Dispose	14
3.7.2	LINQ To SharePoint	15
3.7.3	Client-Objektmodell	15
3.7.4	SharePoint Software Boundaries	15
3.7.5	Code-Performance	15
3.8	Spezifische SharePoint-Bausteine	16
3.8.1	Workflows	16
3.8.2	Webparts	16

3.9	Dokumentation	16
3.9.1	Code-Kommentare	16
3.9.2	Zu erstellende Dokumente	16
3.10	Migration bestehender 2007er-Lösungen auf 2010	17
4	Test und Qualitätssicherung.....	18
4.1	Code Review.....	18
4.1.1	Checkliste Entwurf	18
4.1.2	Checkliste Code	19
4.1.3	Checkliste Dokumentation	20
4.1.4	Checkliste Deployment	20
4.2	Unit Tests.....	21
4.3	Tool-gestützte Tests	21
4.4	Manuelle Tests.....	21
5	Paketierung und Deployment.....	22
5.1	Solution (WSP)	22
5.2	Sandboxed Solutions	22
5.3	GAC- bzw. bin-Installation von Assemblies	22
5.4	Installation von Dateien im SharePoint-Root	22
5.5	Installationsskripte	23
5.6	Upgrade und Löschen von Erweiterungen.....	23
5.7	Übergabe an den Betrieb	23

1 Adressaten und Zielsetzung

Dieses Dokument legt Vorgaben für die Entwicklung und das Deployment von Erweiterungen für die bei Dataport betriebenen SharePoint 2010-Infrastrukturen fest. Es soll die Erstellung **qualitativ hochwertiger** und in Bezug auf sämtliche Phasen ihres Lebenszyklus robuster **SharePoint-Lösungen** fördern.

Adressaten dieses Dokuments sind der Betrieb der SharePoint-Infrastrukturen bei Dataport (TI43) sowie die SharePoint-Entwicklungsabteilung bei Dataport (LI32). Die Vorgaben gelten auch für externe Dienstleister, die durch Dataport oder Kunden der durch Dataport betriebenen SharePoint-Infrastrukturen beauftragt werden. Die Punkte bzgl. Anwendung des SharePoint Designers und Installation von Sandboxed Solutions betreffen auch Site Collection Administratoren.

Dieses Dokument ist für **sämtliche Erweiterungen**, die in den durch Dataport betriebenen SharePoint 2010-Infrastrukturen installiert werden sollen, **verpflichtend anzuwenden**.

Für Erweiterungen, die für SharePoint 2007 erstellt werden, gilt die Vorgängerversion dieses Dokuments.

Dieses Dokument ist kein SharePoint-Entwickler-Tutorial. Es setzt voraus, dass der Leser SharePoint als Entwicklungsplattform beherrscht.

2 Überblick über den Entwicklungs- und Deployment-Prozess

Die Lösungsentwicklung für SharePoint hat **gängigen Vorgehensmodellen des Software Engineerings** zu folgen, um eine möglichst hohe Qualität der ausgelieferten Software sicherzustellen. Dieses Dokument soll dabei kein konkretes Vorgehensmodell vorschreiben, da die Entscheidung für ein bestimmtes iteratives oder nicht-iteratives Verfahren projektspezifisch zu treffen ist. Vielmehr wird auf die zwingende Erfordernis eines strukturierten Vorgehens hingewiesen. Typischerweise werden dabei folgende Phasen durchlaufen:



Die SharePoint-Infrastrukturen verfügen neben der Produktionsumgebung i. d. R. über eine zweistufige **Testumgebung**. Das Deployment von Erweiterungen in der Produktionsumgebung ist erst nach erfolgreichem Test in beiden Vorstufen und Freigabe durch den Betrieb zulässig.

3 Entwicklung

3.1 Entwicklungsumgebung

Die Entwicklung erfolgt auf einer **virtuellen Maschine (VM)**, in der SharePoint 2010 installiert ist. Jeder Entwickler arbeitet auf einer eigenen VM, um gegenseitige Behinderungen beim Deployment und Debuggen auszuschließen. Die Entwicklungs-VM wird als Single Server Installation aufgesetzt. Die Entwicklungs-VMs sind im Detail wie folgt eingerichtet:

- Windows Server 2008 R2, 64bit, Englisch
- Active Directory
- SQL Server 2008 R2
- SharePoint 2010 bzw. SharePoint Foundation 2010
- Visual Studio 2010
- SharePoint Designer 2010
- InfoPath 2010
- Office 2010

3.2 Entwicklungswerkzeuge

3.2.1 Visual Studio 2010

Die Entwicklung für SharePoint 2010 erfolgt mit Visual Studio 2010 und den **Visual Studio 2010 Tools for SharePoint 2010**. Das Zielframework ist auf .NET-Version 3.5 (und nicht 4.0) zu stellen. I. d. R. sollte mit der leeren SharePoint-Project-Vorlage begonnen werden und im Anschluss Item-Templates hinzugefügt werden.

3.2.2 SharePoint Designer 2010

Bei der Verwendung des SharePoint-Designers ist zwischen der Entwicklungs- und der Produktionsumgebung zu unterscheiden.

Der SharePoint Designer kann im Entwicklungsprozess für die Erstellung von Masterseiten, einfachen Workflows etc. verwendet werden. Die erstellten Bausteine müssen zwingend als **WSP deployed** werden.

Der **direkte Zugriff auf Produktiv- und Staging-Umgebungen** mit dem SharePoint Designer ist **unzulässig** und wird durch entsprechende Einstellungen technisch unterbunden. Die Verwendung des SharePoint Designers ist nur in explizit vom Betrieb dafür freigegebenen Umgebungen zulässig (z. B. in der ersten Teststufe). Die erstellten Bausteine können dann via WSP wie oben beschrieben in den Staging- und Produktiv-Umgebungen installiert werden.

3.2.3 InfoPath 2010

InfoPath Formulare können unter 2010 nicht mehr mit Visual Studio, sondern nur noch mit dem InfoPath Client erstellt werden.

3.2.4 Versionsverwaltung

Während der Entwicklung ist zwingend ein Versionsverwaltungssystem einzusetzen, das alle für die Lösung relevanten Dateien beinhalten muss.

3.2.5 Bug Tracking

Für das Bug Tracking wird ein Dataport-spezifisches SharePoint-Site-Template verwendet (Anwendungsdatenbank). Dieses Template stellt unter anderem eine Fehlerliste zur Verfügung.

3.2.6 Developer Dashboard

Das Developer Dashboard ermöglicht eine genaue Beobachtung eigener Komponenten in Bezug auf Fehler und Performance und ist dementsprechend einzusetzen. Spezifische Code-Teile können mit Hilfe von SPMonitoredScope begutachtet werden. Siehe hierzu:

- <http://blogs.msdn.com/b/spses/archive/2010/03/11/sharepoint-2010-logging-improvements-part-2-introducing-developer-dashboard.aspx>
- http://www.wictorwilén.se/Post/Improve-your-SharePoint-2010-applications-with-monitoring-using-SPMonitoredScope.aspx?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+WictorWilén+%28Wictor+Wil%C3%A9n%29

3.2.7 Weitere Werkzeuge

Folgende Werkzeuge werden zusätzlich eingesetzt:

- SharePoint Manager 2010 (<http://spm.codeplex.com/>)
- Reflector (<http://www.red-gate.com/products/reflector/>)
- ULS Viewer (<http://code.msdn.microsoft.com/ULSViewer>)

Weitere Werkzeuge (z. B. Developer Toolbar) können nach Bedarf eingesetzt werden.

3.3 Benennung und Strukturierung von Projekten

3.3.1 Pfadlänge

Die Pfadlänge für Dateien in Visual Studio Solutions ist (betriebssystembedingt) auf ca. 260 Zeichen begrenzt. Die Benennung von Repositories, Solutions und Projects sollte daher einem **Kompromiss zwischen Lesbarkeit und sparsamer Zeichenverwendung** folgen. Namen bzw. Namensbestandteile sind möglichst knapp und präzise zu wählen. Zudem sind die im Folgenden genannten Benennungskonventionen einzuhalten.

3.3.2 Repository-Struktur

Pro Lösung bzw. Projekt wird ein Repository angelegt. Die Benennung erfolgt nach folgendem Schema:

- [CompanyName.]Projektname (bei Projekten)
 - z. B. Dataport.EG-DLRL-FHH
- Sammelbezeichnung für mehrere kleinere Projekte, z. B. Kundenname
 - In diesem Fall werden Unterordner im Repository für jedes Kleinprojekt erstellt

Innerhalb des Repository wird folgende Struktur angelegt:

- branches
- tags
- trunk
 - src
 - Solution-Ordner
 - doc
 - db
 - vendor
 - vendorsrc

3.3.3 Ordner-Struktur in der Entwicklungsumgebung

Sämtliche Projekte liegen unter `c:\Projects`. Unterhalb hiervon gibt es pro Repository einen Unterordner, der den Namen des Repository trägt. Die weiteren Unterordner ergeben sich aus dem Download aus dem Repository.

3.3.4 Visual Studio Solution-Struktur

Pro Lösung bzw. Projekt wird i. d. R. eine **einzige Visual Studio Solution** angelegt. Eine Unterteilung in mehrere Solutions sollte nur aus wichtigen Gründen erfolgen (z. B. für wiederverwendbare Komponenten).

Die Benennung erfolgt anhand des Root-Namespace (z. B. `Dataport.DataportDe`).

3.3.5 Visual Studio Project-Struktur

Pro Lösungsbaustein wird ein Visual Studio Project angelegt. Bei der Unterteilung in Projects sollten folgende **Kriterien** berücksichtigt werden:

- Kapselung von Funktionalität
- Wiederverwendung
- Unterteilung in Assemblies (Kapselung, Deployment Target, ...)
- Unterteilung in WSPs (siehe unten)
- Erleichterung der Teamarbeit

Visual Studio Projects werden **nicht vollqualifiziert**, sondern entsprechend der Namespace-Hierarchie benannt (ohne Root-Namespace). Da die Visual Studio-Automatismen (Project-Name = Default-Namespace = Assembly-Name) hierdurch nicht mehr korrekt greifen, sind nach Anlegen des Projects **folgende Einstellungen manuell zu korrigieren**:

- Anpassen des Assembly Name auf den vollqualifizierten Namen (Project Properties)
- Anpassen des Default Namespace auf den vollqualifizierten Namen (Project Properties)

- Anpassen der Assembly Information auf den vollqualifizierten Namen für den Titel (Project Properties)
- Anpassen des Package Name auf den vollqualifizierten Namen (Package Properties)

Der vollqualifizierte Name wird nach folgendem Schema gebildet:

- CompanyName.TechnologyName/Projektname[.Feature]
 - z. B. Dataport.EG-DLRL-FHH.FormUpload

Innerhalb des Projects sollten Ordner zur weiteren Strukturierung genutzt werden. Als Strukturierungskriterien bieten sich der Artefakttyp oder eine Sortierung nach Komponenten an. Die Ordner sollten möglichst treffend, knapp und nach einheitlichem Schema benannt werden. Diese Ordnernamen schlagen sich im Gegensatz zu Mapped Folders und Feature-Ordnern (siehe unten) nicht beim Deployment nieder.

Werden Dateien in den **SharePoint-Root-Ordner** deployed, sind entsprechende Unterordner, die eindeutig benannt sein müssen, anzulegen. Visual Studio 2010 unterstützt dies beim Anlegen entsprechender Project Items. I. d. R. sollte der vollqualifizierte Name als Ordnername gewählt werden. Bei der Benennung dieser Ordner ist zu beachten, dass die Namen in URLs auftauchen können (z. B. \LAYOUTS\...).

3.3.6 SharePoint Solution (WSP)-Struktur

Solutions werden **vollqualifiziert** benannt.

Dem Automatismus von Visual Studio 2010 folgend sollte pro Visual Studio Project ein WSP erstellt werden. Je nach Struktur der Lösung können aber auch Project-übergreifende WSPs sinnvoll sein.

Bei der Strukturierung in WSPs sollte ein Kompromiss zwischen folgenden Kriterien gefunden werden:

- keine monolithischen WSPs, eher kleinere WSPs (gezieltes Ausrollen gewünschter Funktionalität, einfachere Wiederverwendung, geringer Testaufwand bei Upgrade)
- Nicht zu große Anzahl von WSPs (Abhängigkeiten, Installationsaufwand)

Für die Abbildung von Abhängigkeiten zwischen Solutions sind **Solution Dependencies** zu nutzen.

3.3.7 SharePoint Feature-Struktur

Für die **Benennung** von Features (der Teil, den der Nutzer sieht, z. B. in der Websitesammlungs-Administration) gelten folgende **Vorgaben**:

- Feature Titel sind sprechend zu wählen (kein Aufgreifen des Namespace, deutsche Sprache).
- Der Feature Titel beginnt mit der Zielgruppe gefolgt von einem Doppelpunkt und einem Leerzeichen (z. B. „FHHportal:“, „Dataport.de:“).
- Die Feature Beschreibung ist aussagekräftig zu wählen (deutsche Sprache).
- Es ist ein Feature Icon zu verwenden, das die Zielgruppe deutlich macht.

Feature-Ordner werden **vollqualifiziert** benannt. Da Visual Studio für Feature-Ordner im Standard den Project-Name verwendet, muss die Benennung des **Deployment Path** für jedes Feature in den Properties angepasst werden auf:

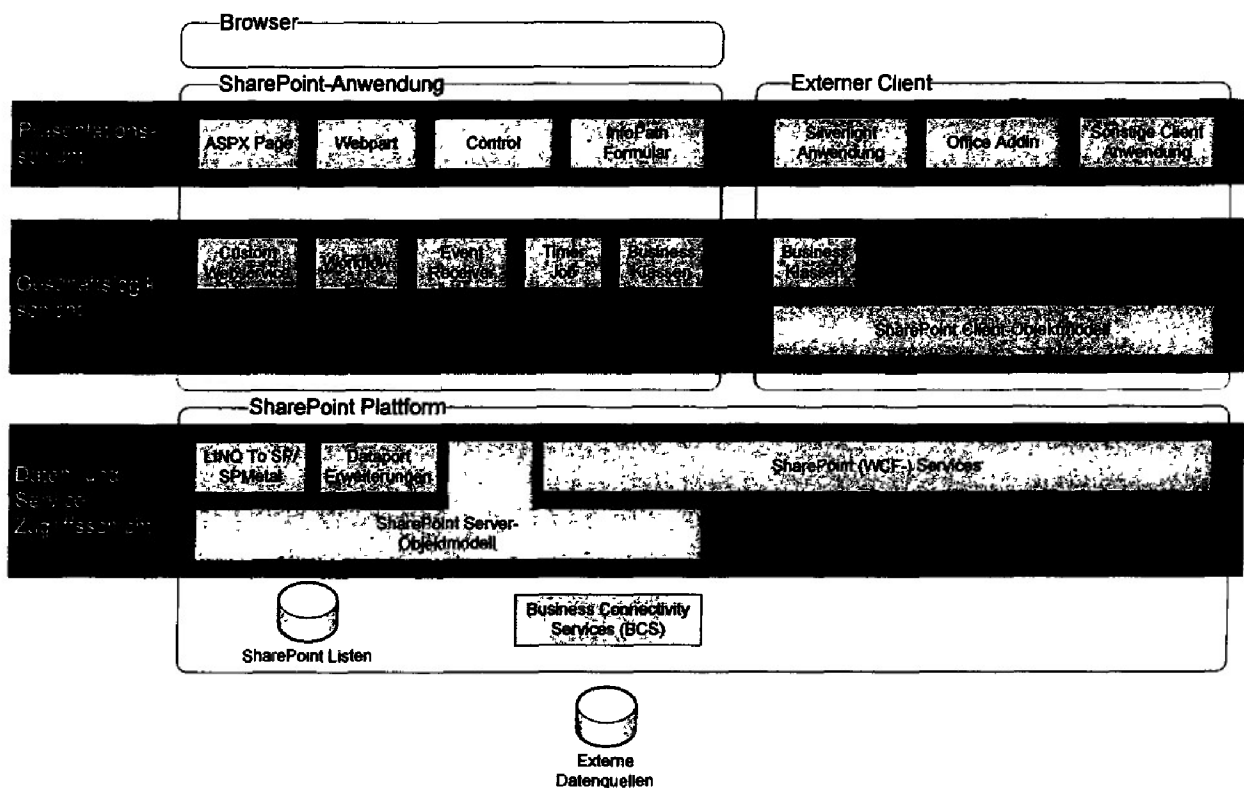
- \$SharePoint.Project.AssemblyFileNameWithoutExtension\$_\$SharePoint.Feature.FileName WithoutExtension\$

Auf diese Weise ist sichergestellt, dass alle Feature-Ordner mit dem Firmennamen beginnen und im SharePoint-Root hintereinander aufgelistet werden.

Ein Feature sollte genau die Elemente beinhalten, die zusammen einen Funktionsbaustein bilden und einen gemeinsamen Scope haben, so dass gewünschte Funktionalität gezielt aktiviert und deaktiviert werden kann. Z. B. sollte das Hinzufügen einer neuen Funktionalität und das Hinzufügen von Content (via Feature) immer in zwei Features aufgeteilt werden. Abhängigkeiten zwischen Features sollten minimiert werden. Eine Ausnahme können „Meta-Features“ bilden, die mehrere kleinere Features aktivieren (vgl. MS Publishing Features).

Für die Abbildung von Abhängigkeiten zwischen Features sind **Feature Activation Dependencies** zu nutzen.

3.4 Softwarearchitektur



Die anzustrebende Architektur für SharePoint-Lösungen folgt einer klassischen Dreischichten-Architektur.

Daten sollten in SharePoint-Listen gehalten werden, sofern keine komplexen Relationen, Transaktionen oder große Datenmengen erforderlich sind. Andernfalls können die Daten in einer eigenen relationalen Datenbank hinterlegt und via BCS eingebunden werden. Externe Datenquellen werden ebenfalls via BCS angebunden. Die Verwendung von BCS ist einer manuell programmierten Anbindung i. d. R. vorzuziehen, da so die BCS-Leistungsmerkmale (CRUD-Formulare, Einbindung in Suche, etc.) genutzt werden können.

Die **Daten- und Service-Zugriffsschicht** wird durch die SharePoint-Plattform bereitgestellt. SharePoint-Anwendungen nutzen das serverseitige Objektmodell, externe Clients die von SharePoint bereitgestellten (WCF-) Services. Der Zugriff auf Daten kann entweder direkt über Listen-Objekte erfolgen oder über die Abstraktionsschicht, die LINQ To SharePoint bzw. SPMetal bereitstellt. Hierdurch wird ein typischerer Zugriff auf Daten und eine komfortable Abfragesyntax ermöglicht.

Für **Logging** und die Verwaltung von **Konfigurationsparametern** stellt Dataport entsprechende Erweiterungen bereit. Diese sind zwingend zu verwenden.

Die **Geschäftslogikschicht** wird für SharePoint-Anwendungen als serverseitiger Code implementiert. Je nach Anforderung stehen verschiedene Erweiterungsschnittstellen (Workflow, Event Receiver, etc.) zur Verfügung. Externe Client-Anwendungen nutzen möglichst das Client-Objektmodell, um den Aufruf der SharePoint Services komfortabel zu kapseln.

Die **Präsentationsschicht** wird für SharePoint-Anwendungen über die aus ASP.Net bekannten Techniken umgesetzt. Client-Anwendungen können z. B. via Silverlight umgesetzt werden, sofern in der Zielumgebung das entsprechende Plugin ausgerollt ist. Silverlight bietet sich insbesondere bei komplexen Anforderungen an die Präsentationsschicht an. Diese sind mit Silverlight i. d. R. einfacher umzusetzen, als mit klassischer Webprogrammierung.

Die Präsentationsschicht ist möglichst strikt von der Geschäftslogik zu trennen, um eine bessere Wart- und Testbarkeit des Codes zu gewährleisten. Code, der Abhängigkeiten gegenüber SharePoint aufweist, ist bestmöglich von der reinen Geschäftslogik zu trennen.

3.5 Allgemeine Programmiervorgaben

3.5.1 Programmiersprache

Für .NET-Code ist ausnahmslos die Programmiersprache **C#** vorgeschrieben.

3.5.2 .NET Framework-Version

.NET-Code ist gemäß aktuellem Stand (April 2011) für das .NET-Framework in der **Version 3.5** zu erstellen.

3.5.3 Code-Konventionen

Code-Konventionen machen verbindliche Vorgaben für den anzuwendenden Programmierstil. Hierunter fallen die Benennung von Bezeichnern, Codeformatierung, etc. Es gelten als Vorgabe die „**Design Guidelines for Developing Class Libraries**“ auf MSDN (<http://msdn.microsoft.com/en-us/library/ms229042.aspx>).

Bzgl. der Codeformatierung gelten insbesondere folgende Regeln:

- Einrückung gemäß Visual Studio Standard
- Klammersetzung: Öffnende Klammern in neue Zeile
- Lange Zeilen umbrechen
- Vermeidung unnötiger Leerzeilen
- Konsistente Formatierung

3.5.4 Programmierung unter SharePoint

SharePoint ist zwar technisch eine ASP.Net-Anwendung, definiert aber ein eigenes Vorgehensmodell für Erweiterungen, das sich von klassischer ASP.Net-Programmierung unterscheidet.

Das **Vorgehensmodell** wird im SharePoint SDK und diversen Quellen (z. B. <http://msdn.microsoft.com/en-us/library/cc537498.aspx>) ausführlich beschrieben und wird daher hier nicht wiederholt. Es umfasst aber insbesondere folgende Aspekte und Regeln:

- Ein eigenes Objektmodell
- Weitmöglichste Ausnutzung von Standard-Funktionalität
- Gezielte Erweiterung über definierte „Schnittstellen“ (z. B. Webparts, Application Pages, Content Types, Custom Actions, etc.)
- Zusammenfassen von Funktionalität in Features
- Deployment ausschließlich via SharePoint Solutions (WSPs)

Dieses Vorgehensmodell ist strikt einzuhalten. Im Umkehrschluss heißt dies, dass **Erweiterungen außerhalb dieses Vorgehensmodells unzulässig** sind, insbesondere:

- Veränderungen an Dateien, die von SharePoint mitgeliefert werden
- Direkter Zugriff (lesend oder schreibend) auf die SharePoint-Datenbanken unter Umgehung des Objektmodells
- Manuelles Deployment von Funktionalität ohne WSPs

Darüber hinaus sind folgende Regeln zu beachten:

- Umsetzung der Erweiterungen mit **möglichst leichtgewichtigen Komponenten** in Bezug auf deren Auswirkung auf die Infrastruktur; so ist die Erstellung von http-Handlern und -Modulen nur nach Rücksprache mit dem Betrieb zulässig
- Erweiterungen sind so zu programmieren, dass sie möglichst einfach auf kommende SharePoint-Versionen **migriert werden können**; so sind z. B. komplexe Site Definitions zu vermeiden, stattdessen sollten minimale Site Definitions in Kombination mit Feature Stapling eingesetzt werden

3.5.5 SharePoint-Version

Die Lösung darf nur Funktionalitäten nutzen bzw. voraussetzen, die auf der jeweiligen Zielplattform vorhanden sind. Im Zweifel ist bereits bei der Konzeptionierung Rücksprache mit dem Betrieb zu nehmen.

Insbesondere ist im Vorfeld zu klären, ob SharePoint Server-Funktionalität genutzt werden darf, oder ob die Lösung auch auf SharePoint Foundation lauffähig sein soll. Bezüglich der SharePoint Server-Funktionalität ist die Unterscheidung zwischen den unterschiedlichen Lizenzvarianten zu beachten. Werden die höherwertigen Varianten benötigt, muss im Vorfeld geklärt werden, ob die entsprechenden **Lizenzen** vorliegen bzw. beschafft werden können.

Stellt die Lösung besondere Ansprüche an den Patch-Level der Infrastruktur ist auch hier im Vorfeld eine Abstimmung mit dem Betrieb erforderlich.

3.5.6 Customized vs Uncustomized

Erweiterungen sind immer als **uncustomized files** zu deployen. Dies gilt auch für sogenannte authored artifacts (z. B. Listen, Master pages, Page layouts, Content types). Direkte Änderungen in den Infrastrukturen (customized files) sind in der Quellcodeverwaltung nicht abgebildet, folgen keinem sauberen Deploymentprozess und verringern die Wartbarkeit und sind daher zu unterlassen.

3.5.7 Interne Klassen

Folgende Klassen sind intern und dürfen nicht für die Programmierung verwendet werden:
<http://msdn.microsoft.com/en-us/library/ee556849%28office.14%29.aspx>.

3.5.8 Fehlerbehandlung

Fehlersituationen sind vom Programmcode zu behandeln. Je nach Schwere des Fehlers und der Fähigkeit des Programms, den Fehler ohne Programmabbruch zu behandeln, sind folgende Aktionen bei der Fehlerbehandlung durchzuführen:

- Programm kann Fehler behandeln (vorhergesehene Fehler)
 - Fehler behandeln
 - ggf. Nachricht an Nutzer ausgeben, ggf. mit Lösungsmöglichkeit
 - im Ablauf fortfahren
- Fehler erfordert Programmabbruch (unvorhergesehene Fehler)
 - Programmablauf stoppen
 - Ressourcen freigeben
 - Logging
 - Rückmeldung an den Nutzer

Für den Umgang mit Exceptions gelten folgende Regeln:

- Exceptions dürfen nur in Ausnahmen bzw. tatsächlichen Fehlersituationen auftreten, sie sind kein Mittel zur Steuerung des Kontrollflusses. So hat z. B. die Prüfung von Eingabewerten rechtzeitig zu erfolgen, so dass Exceptions gar nicht erst auftreten können.
- Es dürften nur solche Exceptions abgefangen werden, mit denen der Programmcode explizit umgehen kann. Das Abfangen generischer Exceptions (z. B. System.Exception) ohne Abbruch des Programms kann zu undefinierten Programmzuständen führen.
- Für das Logging ist Exception.ToString() (enthält Stack-Trace) und nicht Exception.Message zu verwenden.
- An den Nutzer sind einfache und hilfreiche Fehlermeldungen zurückzugeben (z. B. kein Stack Trace).

In SharePoint gelten insbesondere für Webparts weitere Vorgaben:

- Ein Webpart muss seine Fehlerbehandlung autark durchführen und darf keine Exceptions an die aufrufende Seite weiterleiten. Nur so ist sichergestellt, dass ein Fehler in einem Webpart nicht den Aufruf der gesamten Seite verhindert.
- Dementsprechend ist für jede Webpart-Methode, die von der Seite aufgerufen wird (CreateChildControls(), RenderContents(), etc.) ein try/catch-Block vorzusehen.

3.5.9 Logging

Das Logging muss zwingend über die von Dataport bereitgestellte Komponente **Dataport.SharePoint.Common.SPGDeploy** erfolgen. Für diese Komponente existiert eine separate Dokumentation.

3.5.10 Konfigurationsparameter

Konfigurationsparameter müssen zwingend über die von Dataport bereitgestellte Komponente **Dataport.SharePoint.Common.SPGDeploy** verwaltet werden. Für diese Komponente existiert eine separate Dokumentation. Beim Umgang mit Konfigurationsparametern gilt das Prinzip „Convention over Configuration“, d. h. dass nach Möglichkeit Parameter über Konventionen oder aus dem Kontext ermittelt werden oder zumindest entsprechende Standardwerte gelten, die nur bei Bedarf überschrieben werden müssen.

Änderungen an der **web.config** sind nur über eine Solution zulässig (via Objektmodell oder deklarativ nach <http://msdn.microsoft.com/en-us/library/ms439965.aspx>). Manuelle Änderungen sind unzulässig.

3.5.11 Sicherheit

Gängige Vorgaben zur Sicherheit von Webanwendungen sind einzuhalten (siehe z. B. <http://www.sans.org/top25-software-errors/>). Insbesondere ist zu beachten:

- Validierung sämtlichen Inputs (Formulare, Query-Strings, ...)
- Parametrisierte SQL-Abfragen zum Schutz vor SQL-Injection
- HTML-Encode für Input, der in der GUI ausgegeben wird
- Schutz von sensiblen Daten (z. B. keine Abspeicherung in Hidden Fields)
- Exception Behandlung, defensive Programmierung

Der Einsatz von `AllowUnsafeUpdates = true` sowie `SPSecurity.RunWithElevatedPrivileges` sollte vermieden werden bzw. nur in begründeten Ausnahmen und mit großer Sorgfalt erfolgen.

3.5.12 Links

SharePoint-interne Links sind immer relativ anzugeben bzw. es sind Platzhalter oder Eigenschaften aus dem Objektmodell zu verwenden.

3.5.13 Interne Namen

Interne Namen für Listen, Spalten, Inhaltstypen etc. dürfen keine Umlaute, Sonderzeichen und Leerzeichen enthalten.

3.5.14 Browserkompatibilität

Erstellte Anwendungen mit GUI-Komponenten sind immer in verschiedenen Browsern zu testen. Sofern nicht andere Anforderungen definiert sind, ist eine korrekte Darstellung in mindestens folgenden Browsern sicherzustellen:

- Internet Explorer 7, 8 und 9
- Firefox 3 und 4

3.5.15 Barrierefreiheit

Erstellte Anwendungen mit GUI-Komponenten müssen gültiges XHTML erzeugen. Weitergehende Anforderungen an die Barrierefreiheit sind projektspezifisch.

3.5.16 Lokalisierung

Sollte eine Lokalisierung einer Anwendung in verschiedene Sprachen bzw. Kulturen erforderlich sein, sind die entsprechenden Mechanismen unter SharePoint zu nutzen (ressource files).

3.5.17 Reservierte Query String-Parameter

Bestimmte Query String-Parameter sind reserviert für die SharePoint-interne Verwendung. Sie dürfen daher nicht als Namen von eigenen Parametern verwendet werden. Siehe hierzu:

http://blogs.technet.com/b/stefan_gossner/archive/2009/01/30/querysting-parameters-you-should-not-use-in-your-sharepoint-application.aspx

3.5.18 Versionsverwaltung

Pro Release wird ein Tag erstellt mit der Benennung REL-<releasenummer>.

Branches werden nur erstellt, wenn dies zwingend erforderlich ist. Es werden i. d. R. Release- bzw. Bugfix-Branches gebildet, keine Feature-Branches. Die Änderungen in den Branches müssen entsprechend in Trunk gemerged werden.

3.6 Claims

Die bei Dataport eingesetzten Infrastrukturen nutzen neben klassischer Authentifizierung auch Claims-basierte Authentifizierung. Neben der erhöhten Mächtigkeit im Bereich Authentifizierung bringt die Verwendung von Claims unter SharePoint einige Funktionseinschränkungen für spezifische Komponenten mit sich. Zudem sind bei der Programmierung einige Besonderheiten zu beachten, um eine Kompatibilität des Codes sowohl zu Claims als auch zu klassischer Authentifizierung zu gewährleisten.

3.6.1 Funktionseinschränkungen durch Claims

Folgende SharePoint-Funktionen sind beim Einsatz von Claims Einschränkungen unterworfen (Stand: April 2011):

- PowerPivot
 - PowerPivot wird nur im Classic Mode voll unterstützt.
- Visio Services, Excel Services, Performance Point Services, InfoPath Services
 - Müssen Berechtigungen des angemeldeten Nutzers an das Datenbank Backend delegiert werden (z.B. für eine Abfrage der Form "Gebe mir Daten, die für Anwender xxx relevant sind") funktioniert dies nur im Windows-Claims Mode (nicht bei FBA / SAML, usw.) Für externe Anwender bedeutet dies ggf. eine Beschränkung.
- SQL Server 2008 R2 Reporting Services
 - Reporting Services selbst ist nicht Claims-aware, somit können bei Claims-basierter Authentifizierung die Berechtigungen nicht an das Datenbank-Backend weitergegeben werden.
 - Alternative: Fest hinterlegte Credentials für den Backend-Zugriff (SSRS DataSources). Anfragen der Form "Gebe mir Daten, die für Anwender xxx relevant sind", wobei xxx über die Credentials ermittelt werden, sind also nicht möglich.
 - <http://technet.microsoft.com/en-us/library/ff487970.aspx>
 - <http://blogs.msdn.com/b/psssql/archive/2011/02/24/sharepoint-adventures-why-isn-t-claims-working-with-ssrs.aspx>
- People Picker
 - Externe Anwender werden nicht validiert, d. h. Tippfehler bei der Eingabe eines Namens z. B. zum Erteilen einer Berechtigung werden nicht erkannt.
- Audiences
 - Audiences für externe Anwender (SAML Claims) werden ohne Zusatzmaßnahmen nicht funktionieren. Für die entsprechenden Anwender müssen vor allem die Profile

erzeugt werden, sofern externe Anwender mit Audiences arbeiten sollen (entweder mit eigenen Skripten oder manuell).

- <http://blogs.technet.com/b/speschka/archive/2010/06/12/using-audiences-with-claims-auth-sites-in-sharepoint-2010.aspx>

- **RSS Feed Web Part**

- Sofern das RSS Feed Web Part Inhalte aus SharePoint-Listen konsumiert, gibt es Einschränkungen. Unter Claims funktioniert das RSS Feed Webpart nur, wenn der Anwender über Kerberos angemeldet wird. Für interne Anwender, die über NTLM per UAG auf die Seite gelangen oder externe Anwender, die per ADFS und SAML angemeldet werden, steht die Funktionalität nicht zur Verfügung, sondern es gibt eine Fehlermeldung.

3.6.2 Programmiervorgaben für den Umgang mit Claims

3.6.2.1 Allgemeine Vorgaben

Erstellter Code muss sowohl unter **klassischer Authentifizierung** als auch unter **Claims-basierter Authentifizierung lauffähig** sein. Ggf. sind entsprechende Fallunterscheidungen bzgl. des Authentifizierungsproviders (Claims oder Classic Mode, siehe unten) zu verwenden.

Der Code ist bereits in der Entwicklungsumgebung jeweils in einer Webanwendung mit und ohne Claims-basierter Authentifizierung zu **testen**. Entwickler müssen dabei folgende **Szenarien** berücksichtigen:

- Windows integrierte basierte Claims-Authentifizierung (interne Anwender, die von intern oder extern zugreifen)
- Claims-Authentifizierung über ADFS und Security Assertion Markup Language (SAML) für externe Anwender, die auf den internen SharePoint zugreifen
- Ggf. zukünftig Claims und Forms Based Authentication

Gleichwohl kann in der Entwicklung nicht die komplette Authentifizierungsinfrastruktur aus der Produktion nachgebildet werden. Entsprechende weitergehende Tests müssen daher in den der Produktion vorgelagerten Testumgebungen erfolgen.

Da für die Programmierung mit Claims unter SharePoint derzeit noch keine abschließenden Empfehlungen von Microsoft verfügbar sind, stellen die im Folgenden genannten Hinweise nur den aktuellen Stand dar und sind ggf. nicht vollständig. Dementsprechend kommt dem **Test** der erstellten Komponenten im Claims-Umfeld eine noch höhere Bedeutung zu. Dies sollte im Entwicklungs- und Projektzeitplan entsprechend berücksichtigt werden.

3.6.2.2 Login-Namen

Login-Namen folgen unter Claims der **veränderten Notation** `i:0#.w|domain\username`. Die genaue Notation hängt dabei vom zu Grunde liegenden Provider ab. Die Beispiele gehen von Windows integrierter Authentifizierung aus.

```
string loginName = SPContext.Current.Web.CurrentUser.LoginName; // i:0#.w|sp2010dev\testuser
```

Wird im Code direkt mit Login-Namen der Notation `domain\username` gearbeitet, führt dies beim Umstieg auf Claims zu Fehlern. **Manuelles Parsen bzw. Erstellen von Login-Namen** ist daher zu **vermeiden**. Stattdessen sollte mit den entsprechenden Properties (z. B. `SPUser.LoginName`) gearbeitet werden.

```
SPUser spUser = web.AllUsers["@sp2010dev\testuser"]; //funktioniert nicht(!)
```

```
SPUser spUser2 = web.AllUsers[loginName]; //funktioniert
```

Ist eine direkte Arbeit mit Login-Namen erforderlich, stellt die Klasse `SPClaimProviderManager` (<http://msdn.microsoft.com/en-us/library/microsoft.sharepoint.administration.claims.spclaimprovidermanager.members.aspx>) zwei Methoden für die Konvertierung zur Verfügung. `DecodeClaim()` wandelt einen Claim-String in ein `SPClaim`-Objekt um, das über die Value-Property wiederum den Zugriff auf den (dekodierten) Login-Namen ermöglicht:

```
string encodedClaim = SPContext.Current.Web.CurrentUser.LoginName;//i:0#.w|sp2010dev\testuser
string decodedClaim = null;
SPClaimProviderManager claimManager = SPClaimProviderManager.Local;
if (claimManager != null)
{
    SPClaim claim = claimManager.DecodeClaim(encodedClaim);
    decodedClaim = claim.Value; //sp2010dev\testuser
}
```

`EncodeClaim()` wandelt ein `SPClaim`-Objekt in einen Claim-String um:

```
string decodedClaim = @"sp2010dev\testuser";
string encodedClaim = null;
SPClaimProviderManager claimManager = SPClaimProviderManager.Local;
if (claimManager != null)
{
    SPClaim claim = new SPClaim(SPClaimTypes.UserLogonName, decodedClaim,
        "http://www.w3.org/2001/XMLSchema#string",
        SPOriginalIssuers.Format(SPOriginalIssuerType.Forms, "myprovider"));
    encodedClaim = claimManager.EncodeClaim(claim); // i:0#.w|sp2010dev\testuser
}
```

Speichert eine Komponente Login-Namen zwischen (z. B. in XML-Dateien oder einer Datenbank) müssen diese Login-Namen beim Umstieg auf Claims durch entsprechende Maßnahmen (z. B. Powershell-Skript) migriert werden.

3.6.2.3 Fallunterscheidung zwischen Claims und klassischer Authentifizierung

Um die korrekte Ausführung von Code sowohl in Claims-basierten als auch in klassisch-authentifizierten Webanwendungen zu gewährleisten, kann eine Fallunterscheidung erforderlich sein. Die Klasse `SPClaimProviderManager` bietet hierfür die statische Methode `IsClaimsUser()`, die prüft, ob der aktuelle Nutzer ein Claims-basierter Nutzer ist:

```
if (SPClaimProviderManager.IsClaimsUser())
{
    //Claims-basierte Authentifizierung behandeln
}
else
{
    //klassische Authentifizierung behandeln
}
```

Für andere als den aktuellen Nutzer kann auf die Implementierung des `IClaimsPrincipal`-Interface geprüft werden:

```
IClaimsPrincipal claimsPrincipal = principal as IClaimsPrincipal;
if (claimsPrincipal != null)
{
    //Claims-basierte Authentifizierung behandeln
}
```

```
else
{
    //klassische Authentifizierung behandeln
}
```

3.6.2.4 Ermittlung des Claim-Issuers

Erfordert der Code eine Fallunterscheidung nach der (**Authentifizierungs-**) **Herkunft** des Nutzers (z. B. Windows-Nutzer vs. FBA), kann diese Herkunft bei Claims wie folgt ermittelt werden:

```
SPClaimProviderManager claimManager = SPClaimProviderManager.Local;
if (claimManager != null)
{
    SPClaim userClaim =
        claimManager.DecodeClaim(SPContext.Current.Web.CurrentUser.LoginName);
    SPOriginalIssuerType issuerType =
        SPOriginalIssuers.GetIssuerType(userClaim.OriginalIssuer);
    string issuerIdentifier =
        SPOriginalIssuers.GetIssuerIdentifier(userClaim.OriginalIssuer); //ID

    if (issuerType == SPOriginalIssuerType.Windows)
    {
        //...
    }
    else if (issuerType == SPOriginalIssuerType.Forms)
    {
        //...
    }
}
```

3.6.2.5 SPUser-Objekte

Nutzer werden unter SharePoint als SPUser-Objekt repräsentiert. Dies gilt sowohl bei Claims-basierter Authentifizierung als auch bei klassischer Authentifizierung. In Bezug auf den Umgang mit dem SPUser-Objekt sind beim Umstieg auf Claims (mit Ausnahme der Login-Namen, siehe oben) derzeit keine Besonderheiten bekannt.

3.6.2.6 RunWithElevatedPrivileges

SPSecurity.RunWithElevatedPrivileges kann bei einigen Aufrufen Probleme unter Claims verursachen. Diese Probleme scheinen nur unter Forms Based Authentication aufzutreten.

3.6.2.7 Zugriff auf externe Ressourcen

Beim Aufruf externer Ressourcen (z. B. Web Services) ist bei der Übergabe der Anmeldeinformationen darauf zu achten, ob die Ressourcen mit Claims umgehen können („Claims-aware“). Andernfalls sind die Anmeldeinformationen unter Verwendung der oben genannten Methode DecodeClaim() zu übergeben.

3.7 Performance

3.7.1 Dispose

Bei der Programmierung ist auf eine ordnungsgemäße Zerstörung von nicht mehr benötigten Objekten mittels Dispose bzw. using zu achten. Vor Auslieferung ist der Code mit **SPDisposeCheck**

zu überprüfen. Auskunft hierüber geben folgende Dokumente (auf entsprechende Aktualisierungen der Dokumente für SharePoint 2010 ist zu achten):

- <http://msdn.microsoft.com/en-us/library/ee557362%28office.14%29.aspx>
- <http://blogs.msdn.com/rogerla/archive/2009/11/30/sharepoint-2007-2010-do-not-dispose-guidance-spdisposecheck.aspx>
- <http://blogs.msdn.com/rogerla/archive/2008/02/12/sharepoint-2007-and-wss-3-0-dispose-patterns-by-example.aspx>

3.7.2 LINQ To SharePoint

Da LINQ-Abfragen unter SharePoint intern in CAML übersetzt werden und CAML eine geringere Mächtigkeit als LINQ besitzt, ist auf die **Performance von Abfragen** zu achten. Ineffiziente (und nicht unterstützte) Abfragen, sind zu vermeiden. Siehe hierzu <http://msdn.microsoft.com/en-us/library/ee536585%28office.14%29.aspx>.

3.7.3 Client-Objektmodell

Bei der Programmierung mit dem Client-Objektmodell ist auf eine **Minimierung der Roundtrips** zum Server zu achten.

3.7.4 SharePoint Software Boundaries

Die **Größenbeschränkungen** bzw. –empfehlungen für spezifische SharePoint-Objekte (z. B. Listeneinträge pro Ordner, Größe von Datenbanken, etc.) sind zwingend zu beachten. Siehe hierzu <http://technet.microsoft.com/de-de/library/cc262787.aspx>

Darüber hinaus sind die maximale URL-Länge von 260 Zeichen

- <http://blogs.msdn.com/b/joelo/archive/2007/06/27/file-name-length-size-and-invalid-character-restrictions-and-recommendations.aspx>
- <http://www.lcbridge.nl/download/limitsurl.htm>

und die unzulässigen Zeichen in URLs zu beachten:

- <http://support.microsoft.com/default.aspx?scid=kb;en-us;905231>

3.7.5 Code-Performance

Bei der Programmierung ist auf die Erstellung von performantem Code zu achten. Insbesondere sollte die Erstellung unnötiger Objekte sowie der Gebrauch von Schleifen/Indexer mit vielen Elementen vermieden werden.

Die Auswirkungen des Codes bei mehrfachen Aufrufen durch eine Vielzahl von Nutzern ist zu beachten (z. B. bei Navigationselementen). Ggf. sind Caching-Mechanismen (SharePoint-Mechanismen oder ASP.Net) einzusetzen.

Eine gute Übersicht zu beachtender Punkte liefern:

- <http://msdn.microsoft.com/en-us/library/bb687949.aspx>
- <http://msdn.microsoft.com/en-us/library/ee558807%28office.14%29.aspx>.

3.8 Spezifische SharePoint-Bausteine

3.8.1 Workflows

Workflows sollten nicht zu spezifisch entwickelt werden, damit ihre Wiederverwendbarkeit gewährleistet bleibt. Sie müssen robust gegenüber ihrem Einsatz in einem „falschen“ Kontext sein.

3.8.2 Webparts

Webparts müssen als WSS-V3-Webparts erstellt werden, d. h. sie müssen von `System.Web.UI.WebControls.WebParts.WebPart` erben.

3.9 Dokumentation

3.9.1 Code-Kommentare

Code ist sinnvoll zu kommentieren. Für die Kommentierung der API (Klassen, Methoden, Properties) wird die Verwendung der Syntax für **XML-Kommentare** vorgeschrieben.

Für sonstige Kommentare wird die normale Kommentar-Syntax verwendet. Kommentare sind sinnvoll einzusetzen. Sie sollen nicht das Offensichtliche kommentieren, sondern dem lesenden Entwickler nützliche Hinweise geben, die ein schnelles Verständnis des Codes fördern. Kommentare sind durchgängig in Deutsch oder Englisch und mit Sorgfalt in Bezug auf die Vermeidung von Rechtschreibfehlern zu verfassen.

3.9.2 Zu erstellende Dokumente

Jede Anwendung ist zu dokumentieren. Die Dokumentation muss folgende Dokumente umfassen:

- **Benutzerdokumentation**
 - Die Benutzerdokumentation richtet sich an den späteren Anwender des Programms.
 - Sie erklärt im Detail die Bedienung der einzelnen Funktionen des Programms.
 - Sofern sinnvoll, sind zur Veranschaulichung Screenshots zu verwenden.
 - Eine Gliederung ist nicht vorgeschrieben, da sie für das jeweilige Programm sinnvoll festzulegen ist. I. d. R. empfiehlt sich aber eine Untergliederung anhand der unterschiedlichen Rollen und ein problemorientierter Ansatz.
- **Betriebsdokumentation**
 - Die Betriebsdokumentation richtet sich an die Administratoren, die das Programm installieren und betreiben.
 - Der Betrieb stellt eine Vorlage für die Betriebsdokumentation bereit, die zwingend zu verwenden ist.
 - Sie muss folgenden Mindestinhalt umfassen:
 - Beschreibung der Funktionalität/Einführung
 - Beschreibung der Komponenten/Bestandteile (Solutions, Features) inkl. Auflistung der durch die Solutions bzw. Features vorgenommenen Operationen (Kopieroperationen, web.config-Einträge, Feature Receiver, etc.)
 - Installationsvoraussetzungen (SharePoint Foundation/Server, .net Version, ...)
 - eventuelle Abhängigkeiten (Solutions, DLLs, ...)

- Installationsanleitung (Vorbereitung, Installation, Aktualisierung, Deinstallation)
- ggf. Hinweise zum Test/Kontrolle der erfolgreichen Installation
- Testfälle
- Dokumentation der vom Entwicklungsteam durchgeführten Tests
- Konfiguration und Betrieb (Konfigurationsparameter/Einstellungsmöglichkeiten, Möglichkeit der Überwachung (Logging, Trace, Performance Counter), ...)
- Eine Übersicht zu Releases/Versionsnummern und deren Unterschieden
- **Entwicklerdokumentation**
 - Die Entwicklerdokumentation richtet sich an den Entwickler, der das Programm wartet oder weiterentwickelt.
 - Sie muss folgenden Mindestinhalt umfassen:
 - Beschreibung der Funktionalität/Einführung
 - Dokumentation der Anforderungsanalyse (Anforderungsdokumente, Fachkonzept etc.)
 - Dokumentation des Entwurfs
 - insbesondere ein Dokument aus dem die Architektur der Anwendung, ihre Komponenten und deren Zusammenspiel, die Anbindung an Drittsysteme etc. hervorgeht
 - Textliche Beschreibungen komplexer Zusammenhänge sind durch geeignete grafische Darstellungen (z. B. UML: Klassendiagramm, Sequenzdiagramm, ...) zu ergänzen
 - werden eigene Datenbanktabellen verwendet, ist deren Datenmodell zu dokumentieren (ERM oder vergleichbare Notation)
 - Hinweise zur Implementierung
 - Bestandteile der Entwicklungsumgebung
 - Erläuterung der Visual Studio Solution- und Projekt-Struktur
 - Programmspezifische Hinweise zur Programmierung; ggf. mit Verweis auf verwendete Anleitungen/Bücher
 - Dokumentation der Tests
 - Dokumentation des Deployments
 - Hinweise zur Paketierung
 - Hinweise zur Installation (i. d. R. Verweis auf die Betriebsdokumentation)

3.10 Migration bestehender 2007er-Lösungen auf 2010

Erweiterungen, die für SharePoint 2007 erstellt wurden, sind prinzipiell auch unter 2010 lauffähig. Das API ist rückwärtskompatibel. Trotzdem sind einige Punkte zu beachten:

- **Neukompilierung**
 - Code, der im IIS läuft, muss nicht neu kompiliert werden. Für anderen Code (Timer Jobs, Event Receiver, Workflows, Feature Receiver, etc.) muss die Referenz auf die Microsoft.SharePoint.dll aktualisiert und der Code neu kompiliert werden.

- **Deprecated types and methods beachten**
 - <http://code.msdn.microsoft.com/sps2010deprecated>
- **Veraltete Bausteine/Funktionalitäten**
 - Site templates (STPs)
- **Abfragengröße**
 - Bei Abfragen im Code, die mehr als 5000 Items zurückliefern (können), muss die Anfrage entweder angepasst werden, oder aber der Threshold heraufgesetzt werden.
- **UI-Änderungen**
 - Änderungen an CSS, Masterpages etc. sind i. d. R. neu aufzusetzen, da die Komponenten in 2010 tiefgreifend überarbeitet wurden.
- **Custom Actions**
 - Durch die Einführung der Ribbon-Oberfläche, ist die Platzierung von Custom Actions zu überprüfen und ggf. anzupassen.
- **Entwicklungswerkzeug**
 - Für 2007er Lösungen wurde i. d. R. WSPBuilder zur Paketierung verwendet. Eine Umstellung auf die Visual Studio SharePoint Tools ist i. d. R. nicht sinnvoll bzw. gerechtfertigt. Die Lösungen werden daher weiterhin mit dem WSPBuilder paketiert.

Weitere Detailinformationen zu den genannten Punkten liefert <http://msdn.microsoft.com/en-us/library/ee662217%28office.14%29.aspx>.

4 Test und Qualitätssicherung

4.1 Code Review

Code Review ist ein Mittel, um nach Abschluss der eigentlichen Programmierarbeiten anhand des Codes die Einhaltung von Regeln zu untersuchen und ggf. Optimierungspotentiale im Code zu identifizieren. Der Schwerpunkt beim Code Review liegt auf:

- Einhaltung des Vorgehensmodells zur Programmierung unter SharePoint
- Einhaltung von Namenskonventionen und Coding-Standards
- Konsequente Anwendung von Dispose/using
- Performance-Optimierung
- Fehlerbehandlung

Das Code Review wird von Entwicklern durchgeführt, die nicht als Programmierer im Projekt tätig waren.

Extern entwickelte Komponenten werden vor ihrer Installation zwingend einem Code Review unterzogen. Als Basis dienen dabei folgende Checklisten:

4.1.1 Checkliste Entwurf

Vorgabe	Erfüllt?	Bemerkung
SharePoint-Erweiterungsmodell		

eingehalten
Ausnutzung von Standard-Funktionalität
Kein Überschreiben von Standard-Dateien
Kein direkter Zugriff auf SP-Datenbanken
Lösung migrationsfreundlich programmiert
Lösung verständlich und wartbar
Lösung für Betrieb in Server-Farm ausgelegt
Sinnvolle Klassenstruktur
Sinnvolle Feature-Struktur und -Scopes
Feature(-Receiver) ziehen bei Deaktivierung Änderungen zurück
Namenskonventionen für Solutions und Features eingehalten
Namenskonventionen für SharePoint-Root-Ordner eingehalten
SharePoint Software Boundaries eingehalten
Keine Konflikte zu anderen Lösungen erkennbar

4.1.2 Checkliste Code

Vorgabe	Erfüllt?	Bemerkung
Programmiersprache C#		
Eindeutige Namespaces		
Namenskonventionen für Klassen und Member eingehalten		
Sinnvolle Code-Kommentare		
Code korrekt formatiert		

Korrektes Dispose (SPDisposeCheck + manuell)

Elevation nur in begründeten Ausnahmen

AllowUnsafeUpdates nur in begründeten Ausnahmen

Keine negativen Performance-Auswirkungen (umfangreiche foreach-Durchläufe etc.)

Korrekte Fehlerbehandlung

Verwendung der zentralen Komponenten für Logging und Konfigurationsparameter

Sicherheitslücken vermieden

Keine Verwendung interner Klassen

Code im Release-Mode kompiliert

Nur benötigte Assemblies referenziert

Code ist unter Claims- und klassischer Authentifizierung lauffähig

4.1.3 Checkliste Dokumentation

Vorgabe	Erfüllt?	Bemerkung
Betriebsdokumentation vollständig		
Entwicklerdokumentation vollständig		

4.1.4 Checkliste Deployment

Vorgabe	Erfüllt?	Bemerkung
Lösung liegt als eine oder mehrere Solutions vor		
Powershell-Installationsskripte liegen vor		

Keine manuellen
Installationsschritte erforderlich,
die sinnvoll automatisierbar
wären

Anwendungsdatenbank
vollständig ausgefüllt

Solution-Manifest in Ordnung
(keine unnötigen Einträge...)

4.2 Unit Tests

Unit Tests unter SharePoint sind i. d. R. nur aufwändig und mit spezifischen Tools umzusetzen, die das Stubbing der verwendeten SharePoint-Objekte ermöglichen.

Die Verwendung von Unit Tests wird daher derzeit nicht vorgeschrieben.

4.3 Tool-gestützte Tests

Tool-gestützte Tests (z. B. für UI-Tests, Lasttests) sollen nach Möglichkeit eingesetzt werden.

4.4 Manuelle Tests

Manuelle Tests sind der wichtigste Baustein für die Qualitätssicherung von SharePoint-Lösungen. Sie sind zwingend vorgeschrieben und müssen dokumentiert werden. Die Tests werden in der Entwicklungs-, sowie in der Test- und in der Staging-Umgebung durchgeführt. Tests werden auf Basis von Testfällen durchgeführt. Die erwarteten Erfolgskriterien für die Tests sind im Vorfeld festzulegen.

Zu testen sind insbesondere:

- Funktionalität
 - Abdeckung der Anforderungen
 - Browserkompatibilität
 - Test unter SharePoint Foundation und SharePoint Server (sofern gefordert)
 - Test mit aktuellem Patch-Level
 - Test unter Belastung (viele Daten, viele Nutzer gleichzeitig)
 - Test in einer Farmumgebung (im Gegensatz zu einer Single Server-Installation)
 - Test mit anonymem Zugriff (sofern gefordert, z. B. bei Internet-Auftritten)
 - Berechtigungen
 - Test mit minimalen Berechtigungen (funktioniert das Programm entsprechend den Anforderungen?)
 - Test mit verschiedenen Rollen/Berechtigungen (haben Rollen Zugang zu den erlaubten Funktionen und keinen Zugang zu nicht erlaubten Funktionen?)
- Performance
 - Entsprechen die Antwortzeiten der Anwendung den Anforderungen? (Anmerkung: Ein Test in der Testumgebung hat hier ggf. beschränkte Aussagekraft)
- Fehlerbehandlung

- Bewusste Eingabe von falschen Daten (leere Eingaben, zu lange Eingaben, Sonderzeichen etc.); fängt das Programm die falschen Eingaben ab und gibt sinnvolle Fehlermeldungen aus?
- Sicherheit (Authentifizierung, Authorisierung)
- Eine gute Checkliste bietet die „Sample code acceptance checklist“ unter <http://technet.microsoft.com/en-us/library/cc707802.aspx>.
- Für bestimmte Lösungen existieren besondere Testkriterien. Insbesondere für Webparts ist die folgende Checkliste zu beachten: <http://msdn.microsoft.com/en-us/library/bb985502.aspx>.
- Deployment
 - Installation der Solution
 - Deinstallation der Solution (Prüfung auf vollständiges Entfernen aller Bestandteile)
- Dokumentation
 - Benutzer-, Betriebs- und Entwicklerdokumentation testen

5 Paketierung und Deployment

5.1 Solution (WSP)

SharePoint-Lösungen müssen zwingend als **WSP** ausgeliefert werden. Weder direkte Kopieroperationen auf den Servern der Farm noch die Installation von Features ohne eine Kapselung in eine Solution sind zulässig. Allein über Solutions ist eine automatische Synchronisation der Server sowie eine vollständige Deinstallation erreichbar.

5.2 Sandboxed Solutions

Abhängig von den Anforderungen ist zu prüfen, ob eine Solution als Sandboxed Solution erstellt werden kann. Sandboxed Solutions sind insbesondere dann nicht geeignet, wenn

- die Umsetzung der Anforderungen zwingend eine Farm Solution erfordert (z. B. Timer Job)
- oder die Solution eine allgemeingültige, Site Collection-übergreifende Erweiterung ist, die Farm-weit zur Verfügung stehen soll.

Sollten für eine Sandboxed Solution stellenweise Farm Solution-Rechte erforderlich sein, sollte nur dieser Bereich in einen Full Trust Proxy ausgelagert und dann aus der Sandboxed Solution aufgerufen werden.

Site Collection Administratoren wird nicht das Recht gewährt, Sandboxed Solutions zu installieren. Das Deployment erfolgt stattdessen, analog zu Farm Solutions, über den Betrieb.

5.3 GAC- bzw. bin-Installation von Assemblies

Assemblies werden je nach Anforderung der Erweiterung im GAC oder im bin-Ordner installiert.

5.4 Installation von Dateien im SharePoint-Root

Dateien, die in den SharePoint-Root-Ordner deployed werden, müssen in den vorgesehenen Standard-Ordern abgelegt werden (z. B. CONTROLTEMPLATES, IMAGES, etc.). Unterhalb dieser Ordner muss immer ein lösungsspezifischer Unterordner angelegt werden.

5.5 Installationsskripte

Die Installation von Lösungen muss komplett automatisiert via Power Shell-Skript erfolgen („One Click Deployment“). Manuelle Schritte dürfen nur in begründeten Ausnahmen erforderlich sein.

Für die Erstellung der Skripte stellt Dataport eine Power Shell-Methodensammlung bereit (Dataport.SharePoint.Powershell.CommonDeploy.ps1).

Pro Solution sind folgende Skripte zu erstellen:

- Install/Update
- Uninstall

Besteht eine Lösung aus mehreren Solutions ist für Install, Uninstall und Update auch jeweils ein Masterskript bereitzustellen, das die einzelnen Skripte der Solutions aufruft.

Sind für unterschiedliche Umgebungen unterschiedliche Installationsparameter erforderlich (z. B. URLs), so ist jeweils ein Skript pro Umgebung zu erstellen.

5.6 Upgrade und Löschen von Erweiterungen

Besondere Vorsicht ist bei einem Upgrade oder dem Löschen vorhandener Erweiterungen geboten. Es ist im Vorfeld zu prüfen, welche Auswirkungen die Aktion auf vorhandene Instanzen, die auf der Erweiterung aufsetzen, hat. Eventuelle Gegenmaßnahmen (Feature-Versionierung und –Upgrade, Assemblyversionierung, Binding Redirects, Erstellung eines Neuen Features/Verstecken des alten Features, etc.) sind bereits in der Entwicklung zu berücksichtigen.

5.7 Übergabe an den Betrieb

Im Rahmen eines Installationsauftrags müssen folgende Bestandteile an den Betrieb übergeben werden:

- WSP-Datei(en)
- Power Shell Installationsskript
- Angabe der Zielinfrastruktur
- Angabe, ob Sandbox- oder Farm-Solution
- Betriebsdokumentation inkl. Testfälle und Testdokumentation (siehe Kapitel zur Dokumentation)
- Benutzerdokumentation

Wurde die Software von einem Drittanbieter entwickelt und erfolgt mit der Übergabe in den Betrieb auch eine Übergabe der Wartungsaufgaben an Dataport, sind folgende Bestandteile zusätzlich zu übergeben:

- Quellcode
- Entwickler-Dokumentation

Die Übergabe erfolgt über eine spezielle SharePoint-Site, die sogenannte **Anwendungsdatenbank**. Diese ist für jede Lösung vollständig auszufüllen (Anwendungssteckbrief, Dokumentation, Testfälle, WSP, etc.).

Ein Deployment muss über einen festgelegten **Freigabeprozess** (SharePoint-Workflow) explizit beantragt und genehmigt werden.

Leistungsbeschreibung

Bereitstellung und Administration des Verzeichnisdienstes „Active Directory“ für WiBeS (V1.0)

Version 1.0
von 2013

Inhaltsverzeichnis

Einführung und Grundsätzliches zum Active Directory	3
Leistungsbeschreibung und Umfang der Vereinbarung	3
Servicezeiten und Kunden-Support	4
Verfügbarkeit des Dienstes	4
Change Management.....	4
Sicherheit.....	4
Kennwort- und Kontensperrungs-Richtlinien.....	4
Verantwortlichkeiten	5
Verantwortung Leistungserbringer	5
Verantwortung Leistungsempfänger	5
Benutzer- und Gruppenverwaltung.....	5
Namenskonventionen für Benutzerobjekten	6
Referenzierte und mitgeltende Dokumente	6

Einführung und Grundsätzliches zum Active Directory

Das vorliegende Dokument beinhaltet die Leistungsbeschreibung für den Betrieb und der Administration der Active Directory (AD) Domäne „dpaorinp.de“ für Wissensmanagement für Berufliche Schulen in Hamburg (WiBeS).

Das AD ist der Verzeichnisdienst von Microsoft Windows Server. Hiermit wird u.a. die Authentifizierung und Autorisierung innerhalb von Microsoft Infrastrukturen durchgeführt und gewährleistet.

Mit Hilfe von Organisationseinheiten (Organizational Units, OUs) können Strukturen gegliedert, Objekte gruppiert und Aufgaben delegiert werden. Innerhalb einer OU-Struktur können unterschiedliche Objekte wie beispielsweise Benutzer, Gruppen, Drucker, Computer, und Server und deren Eigenschaften angelegt und verwaltet werden.

In der AD Domäne „dpaorinp.de“ werden u.a. Verfahren für Dataport-Kunden bereitgestellt. Jeder nutzende Kunde verfügt über einen eigenen OU-Zweig. Die Berechtigungen für die Administration und Verwaltung dieser OUs und der sich darin befindlichen Objekte sind an die jeweiligen Kunden delegiert.

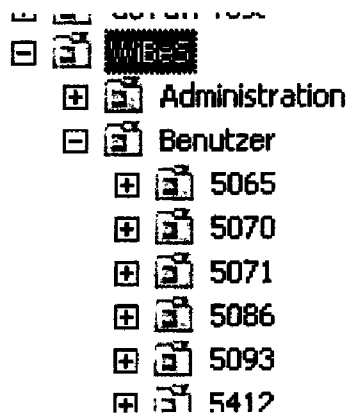


Abbildung 1: Beispielhafte OU-Struktur für Kunden der Domäne „dpaorinp.de“

Leistungsbeschreibung und Umfang der Vereinbarung

Dataport ist Eigner und verantwortlich für den Betrieb der AD Gesamtstruktur. Die technische Umsetzung des Betriebs und der Administration erfolgt durch Dataport TI 41.

Die AD Domäne „dpaorinp.de“ bietet die Authentifizierungs- und Autorisierungsinfrastruktur für WiBeS. Darüber hinaus dient das AD als zentraler Speicherort für alle WiBeS Benutzerkonten und Sicherheitsgruppen.

Servicezeiten und Kunden-Support

Support-Anfragen erfolgen grundsätzlich per E-Mail an das Postfach „Dataport WiBeS Kundenbetreuung“.

Verfügbarkeit des Dienstes

Das AD und seine Autorisierungs- und Authentifizierungs-Dienste stehen gemäß vereinbartem SLA i.A. permanent zur Verfügung.

Wartungstätigkeiten werden auf Grundlage des implementierten Change-Managements grundsätzlich in dem vereinbarten Wartungsfenster durchgeführt.

Nichtgeplante Wartungstätigkeiten, die zu einer Nicht-Verfügbarkeit der Dienste führen könnten, werden auf Grundlage des implementierten Change-Managements im Rahmen eines Notfall-Changes umgehend durchgeführt.

Change Management

Änderungswünsche am Umfang dieser Leistungsbeschreibung werden ausschließlich über das Dataport Change Management entgegengenommen und dort abgestimmt.

Sicherheit

Maßgeblich für die Sicherheitseinstellungen des ADs sind die

1. „Dataport IT-Sicherheitsrichtlinie“,
2. „Sicherheitskonzept Active Directory-Services“,
3. „Betriebshandbuch für die Gesamtstruktur dpaorinx.de“,
4. „Konzeption IT Grundschutz konformer Windows Betrieb TI 1“

in den jeweils aktuell gültigen Fassungen.

Die Korrektheit der Einstellungen werden jährlich im Rahmen eines Reviews geprüft.

Kennwort- und Kontensperrungs-Richtlinien

Die folgende Tabelle zeigt einen Überblick der Kennwort- und Kontensperrungs-Richtlinien.

Richtlinie	Wert
Passwort Historie	5
Maximales Passwort Alter	90

Minimales Passwort Alter	1
Minimale Passwortlänge	10
Komplexitätsanforderungen	Ja
Umkehrbare Passwortverschlüsselung	Deaktiviert
Kontensperrungsdauer	0
Kontensperrungsschwelle	12
Reset des Kontensperrungszählers	0

Tabelle 1: Kennwort- und Kontensperrungs-Richtlinien

Verantwortlichkeiten

Verantwortung Leistungserbringer

Dataport stellt sicher, dass das AD und die dazugehörigen Autorisierungs- und Authentifizierungsdienste zu den vereinbarten Zeiten und Qualität zur Verfügung stehen und uneingeschränkt genutzt werden können.

Verantwortung Leistungsempfänger

Benutzer- und Gruppenverwaltung

Der Kunde ist für die Benutzer- und Gruppenverwaltung selbst zuständig und fungiert als Ansprechpartner für die eigenen Benutzer.

Die Verwaltung von Benutzerkonten (u.a. Konto anlegen, ändern, entsperren, löschen, Kennwort zurücksetzen) und Sicherheitsgruppen (u.a. Gruppe anlegen, ändern, löschen, Mitgliedschaften ändern) erfolgt durch den Kunden und in den dafür vorgesehenen Kunden-OUs. Der Kunde besitzt innerhalb dieser OUs alle notwendigen Berechtigungen für die Verwaltung der Objekte.

Der Kunde übernimmt die Gesamtverantwortung für „seine“ Benutzerkonten und Sicherheitsgruppen.

Die Benutzerverwaltung erfolgt durch den Kunden und ausschließlich mit Hilfe des von Dataport zur Verfügung gestellten Tools. Dieses Tool ist nicht Bestandteil dieser Leistungsbeschreibung.

Namenskonventionen für Benutzerobjekten

Es gilt das Namenskonzept des AD „stadt.hamburg.de“.

Die Attribute „User logon name“ und der „User logon name (pre-Windows 2000)“ ergeben sich aus den ersten sechs Buchstaben den Nachnamens und der ersten beiden Buchstaben aus dem Vornamen.

Der „User logon name“ und der „User logon name (pre-Windows 2000)“ sind innerhalb einer Domäne eindeutig und können nur einmalig vergeben werden. Bei Namensgleichheit bzw. Kollisionen werden neue Namen analog den Regelungen bei HASI für die Domäne fhhnet.stadt.hamburg.de erzeugt.

Referenzierte und mitgeltende Dokumente

Dieses Dokument enthält Informationen und Zusammenfassungen von Regeln aus den folgenden Dokumenten.

- Dataport IT-Sicherheitsleitlinie
- Sicherheitskonzept Active Directory-Services
- Betriebshandbuch für die Gesamtstruktur „Betriebshandbuch für die Gesamtstruktur dpaorinx.de“
- Namenskonventionen Active Directory Services

Einblicke in die aktuelle Versionen können jederzeit bei Dataport TI 41 angefordert werden.

Anlage 7 zum Vertrag V5378/2300000

Messaging

Leistungsbeschreibung der WiBeS Produktionsumgebung Exchange

Version 1.0
Vom 16.01.2013

verantwortlich: Vorname Name; Kurzzeichen

Version: 1.0 vom: 16.01.2013

Status: Gültig

Aktenzeichen: ggf. eingeben

Schutzstufe: keine Schutzstufe

Zielgruppe: Bitte eingeben

Inhaltsverzeichnis

1	Zielsetzung des Dokuments.....	1
2	Out-of-Scope	1
3	Das Projekt WiBeS	1
4	Organisatorische Regelungen	1
5	E-Mail Dienste	2
5.1	Leistungsumfang Postfach.....	2
5.2	Kontingentregelung.....	2
5.3	Postfächer.....	3
5.3.1	Lehrer / Mitarbeiter.....	3
5.3.1.1	Postfachlimits	3
5.3.2	Schüler.....	3
5.3.2.1	Postfachlimits	3
5.4	Funktionserweiterungen der Postfächer.....	3
5.5	Weitere Dienstleistungen	4
5.6	Organisatorische Schnittstelle.....	4
5.7	Öffentliche Ordner.....	4
6	Allgemeine E-Mail Richtlinien	4
7	Postfix.....	5
8	E-Mail Virenschutz (von und nach extern)	5
8.1	Von extern	6
8.2	Nach Extern	7
9	E-Mail Spamschutz.....	7
9.1	Von extern	7
9.2	Nach Extern	7
10	E-Mail Virenschutz (intern).....	7
11	Leistungsabgrenzung	8

1 Zielsetzung des Dokuments

Das vorliegende Dokument beschreibt die Regelungen, die sich aus der Migration von WiBeS zu Dataport hinsichtlich der Mailinfrastruktur ergeben. Diese sind notwendig, damit zwischen Dataport und dem Kunden Einigkeit über einen ordnungsgemäßen Betrieb nach der Migration gewährleistet werden kann. Die allgemeinen Regelungen sollen allen betroffenen Beteiligten bei Dataport und bei der HIBB bekannt sein und sich daraus eine Grundlage für die zukünftige Zusammenarbeit ergeben.

2 Out-of-Scope

Keine Berücksichtigung in diesem Dokument finden

- eventuell notwendige Client Lizenzen (CAL: Client Access Licences).
- Bedienungsanleitung des Systems.
- Noch zu initiiierende Prozeduren / Verfahren zum Anwender-Support.

3 Das Projekt WiBeS

Das Projekt WiBeS stellt für alle Beruflichen Schulen in Hamburg eine gemeinsame Internet-Plattform zur Verfügung.

- Lehrerinnen und Lehrer
- Schülerinnen und Schüler
- Betriebe und Kooperationspartner

sollen einfach und direkt Dokumente und Informationen austauschen, Unterricht und Projekte absprechen und das schulische Leben organisieren.

Das HIBB (Hamburger Institut für berufliche Bildung) unterstützt die Nutzerinnen und Nutzer durch umfangreiche Schulung und Betreuung.

WiBeS ist ein modernes Wissensmanagement-System und bietet zahlreiche Funktionen für

- Teamarbeit,
- Dokumentenmanagement und
- Kommunikation

Hierfür ist Vertrauen untereinander und auch zum System selbst erforderlich. Daher wird Sicherheit bei WiBeS groß geschrieben. Der Zugang ist mit jedem aktuellen Internet-Browser über eine verschlüsselte, passwortgeschützte Verbindung und nur für registrierte Nutzerinnen und Nutzer möglich.

4 Organisatorische Regelungen

Folgende organisatorische Regelungen sind notwendig, um eine ordnungsgemäße Bearbeitung der Aufträge von WiBeS seitens Dataport zu gewährleisten:

- Benennung einer Fachlichen Leitstelle (eines Koordinators) als Ansprechpartner für Dataport.
- Aufträge an Dataport sind an das Postfach wibes@dataport.de zu richten.

- Die Aufträge sind nur durch die Fachliche Leitstelle oder entsprechend beauftragte Personen an Dataport zu richten. Aufträge von Personen außerhalb dieses Personenkreises werden zur Klärung an die Fachliche Leitstelle weitergeleitet.
- Die Service- und Reaktionszeiten für die Aufträge sind in einem gesonderten SLA hinterlegt.
- Grundsätzlich gilt, dass alle (Administrations-) Aufgaben, die durch die Fachliche Leitstelle oder entsprechend beauftragte Personen durchgeführt werden können, auch von diesen auszuführen ist. Eine Abweichung von dieser Regel und eine damit verbundene Beauftragung an Dataport sind grundsätzlich kostenpflichtig. Auf Wunsch des Kunden erstellt Dataport ein Angebot.

5 E-Mail Dienste

In diesem Abschnitt werden die Services und der Betrieb von Exchange ausschließlich im Rahmen von Sharepoint Lösungen beschrieben.

5.1 Leistungsumfang Postfach

Dataport stellt für die Lehrer, Mitarbeiter und Schüler von WiBeS in der Umgebung Dataport Internet-DataCenter E-Mail-Postfächer bereit. Voraussetzung für die Nutzung sind Anmeldekonto im Dataport Internet-DataCenter, welche bei Dataport im externen AD des UAG (Universal Access Gateway von Microsoft) gehalten werden.

Der Zugang zu den Postfächern wird derzeit nur über die Anmeldung an dem UAG ermöglicht. Es können E-Mails zu externen und internen E-Mail-Adressen versandt und empfangen werden.

Technische Basis des E-Mail Systems ist Exchange 2010. Die Nutzung des E-Mail-Dienstes ist grundsätzlich über Outlook-Web-Access (OWA) mit einem Browser, der von Microsoft unterstützt wird, möglich.

Ein Zugriff per Outlook Client via Outlook Anywhere ist deaktiviert, kann aber durch Auftrag des Kunden durch die Dataport Exchange Administration freigeschaltet werden. Dies gilt nur für Postfächer der Lehrer / Mitarbeiter. Die Anzahl der Benutzer wird im Moment 200 nicht überschreiten. Ein Zugriff per Outlook Client via Outlook Anywhere ist ab der Version Outlook 2007 möglich. Outlook 2003 wird explizit nicht unterstützt.

5.2 Kontingentregelung

Für die Erweiterung von Postfachgrößen der Postfächer von Lehrern und Mitarbeitern wird die sogenannte Kontingentregelung angewandt.

Hierfür wird der Speicherplatzbedarf pro Postfach und die Anzahl der existierenden Postfächer in WiBeS 1x pro Jahr ermittelt und der Kontingentermittlung zugrunde gelegt.

Der Speicherplatzbedarf für das Exchange-System beträgt ca. das 5-fache der realen Postfachinhalte (3 Datenbankkopien, Schattenbereich plus "Overhead"). Der maximale Speicherplatzbedarf pro Postfach mit einer Größe von 250 MB beträgt also $250 \text{ MB} * 5 = 1.250 \text{ MB}$.

Von dem errechneten maximalen Speicherplatzbedarf aller Postfächer steht WiBeS 80 % für die Postfächer zur Nutzung zur Verfügung.

Die Fachliche Leitstelle WiBeS hat die Möglichkeit, einmal monatlich die tatsächliche Belegung der Postfächer abzufragen.

Das CCF wird einmal wöchentlich die Postfachüberschreitungen der Postfächer schriftlich mitteilen. Die Erweiterung erfolgt durch die Dataport Exchange Administration. Aufträge hierfür sind über die Fachliche Leitstelle an das Postfach wibes@dataport.de zu richten.

5.3 Postfächer

Bei Einrichtung eines Postfaches steht dem Nutzer standardmäßig folgender Leistungsumfang zur Verfügung:

5.3.1 Lehrer / Mitarbeiter

- Wiederherstellbarkeit gelöschter Objekte über einen Zeitraum von 14 Tagen durch den User
- Zugriff auf das Postfach über Web-Anwendung "Outlook Web-APP (OWA)"
- Zugriff auf das Postfach über Outlook Anywhere, dies muss gesondert freigeschaltet werden.
- Virenschanning der E-Mails (siehe Punkt 8)
- Basis-Spam-Abwehr durch Regeln auf den externen Postfixes (siehe Punkt 7)
- Anti-Spamscanning der von extern eingehenden E-Mails (siehe Punkt 9)

5.3.1.1 Postfachlimits

- Warnmeldung senden ab: 200 MB
- Senden verbieten ab: 250 MB
- Senden und Empfangen verbieten ab: 250 MB

5.3.2 Schüler

- Wiederherstellbarkeit gelöschter Objekte über einen Zeitraum von 14 Tagen durch den User
- Zugriff auf das Postfach über Web-Anwendung "Outlook Web-APP (OWA)"
- Zugriff auf das Postfach über Outlook Anywhere, dies muss gesondert freigeschaltet werden.
- Virenschanning der E-Mails (siehe Punkt 8)
- Basis-Spam-Abwehr durch Regeln auf den externen Postfixes (siehe Punkt 7)
- Anti-Spamscanning der von extern eingehenden E-Mails (siehe Punkt 9)

5.3.2.1 Postfachlimits

- Warnmeldung senden ab: 20 MB
- Senden verbieten ab: 25 MB
- Senden und Empfangen verbieten ab: 25 MB

5.4 Funktionserweiterungen der Postfächer

Die Postfächer können um folgende Funktionalitäten erweitert werden:

- Lehrer / Mitarbeiter: Erweiterung der Postfachgröße im Rahmen der Kontingentregelung (siehe Punkt 5.2) in Schritten von 250 Mbyte bis zu 1 Gbyte mit Einrichtung einer individuellen Warngrenze.
- Setzen von zusätzlichen Alias Adressen (z. B. durch Heirat) innerhalb der Maildomäne.

-
- Setzen von zusätzlichen Postfachberechtigungen. Dies erfordert zwingend die Zustimmung des Postfachinhabers / Postfachberechtigten.
 - Setzen von Empfangs- und Sendebeschränkungen auf Postfächern oder Verteilerlisten.
 - Freischaltungen der Zugriffe über Outlook Anywhere.

Alle diese Funktionserweiterungen erfolgen durch die Dataport Exchange Administration. Aufträge hierfür sind über die Fachliche Leitstelle an das Postfach wibes@dataport.de zu richten.

5.5 Weitere Dienstleistungen

- Mailenablen von Gruppen zu Verteilerlisten
- Durchführung eines automatisierten / scriptgesteuerten Massenmailversandes - dieser ist kostenpflichtig und wird nach Aufwand berechnet.

Alle diese weiteren Dienstleistungen erfolgen durch die Dataport Exchange Administration. Aufträge hierfür sind über die Fachliche Leitstelle an das Postfach wibes@dataport.de zu richten. Auf Wunsch des Kunden kann vorab ein Angebot über die zusätzliche Dienstleistung von Dataport abgegeben werden.

5.6 Organisatorische Schnittstelle

Die Einrichtung, Bearbeitung und Löschung der Postfächer für Lehrer, Mitarbeiter und Schüler von WiBeS erfolgt durch die von WiBeS benannten Datenpfleger bei dem Kunden über ein WEB-Part, welches auf dem WiBeS Sharepoint zur Verfügung gestellt wird.

5.7 Öffentliche Ordner

In der WiBeS Exchange Produktivumgebung gibt es keine öffentlichen Ordner.

6 Allgemeine E-Mail Richtlinien

Die nachfolgenden E-Mail Richtlinien gelten für alle WiBeS User mit Postfach:

- Die maximale E-Mail Größe beträgt 10 MB. Sie gilt für den internen Versand bzw. Empfang sowie für den Versand bzw. Empfang nach und von extern.
Hinweis: Aufgrund der Protokoll Eigenschaften von SMTP (7-bit ASCII) vergrößert sich eine in Outlook (8-bit) geschriebene eMail entsprechend. Für das hier angegebene Limit von 10 MB zählt die Größe, welche die E-Mail im Mail-Weg per SMTP tatsächlich hat.
- Serverseitige sowie regelbasierte E-Mail Weiterleitungen in Outlook nach extern sind grundsätzlich nicht erlaubt.
- Abwesenheitsmitteilungen aus WiBeS nach intern und extern sind freigeschaltet und können genutzt werden.
- Es sind pro E-Mail maximal 1.000 Empfänger von intern oder extern anschreibbar.
- Es werden nur Mails für bekannte Empfänger angenommen – siehe Punkt 7.

- E-Mails mit Passwortgeschützten ZIP – Files werden nicht gescannt, sondern ungeschannt zugestellt. Die E-Mail wird mit einem Eintrag versehen:

"Der Anhang %FILENAME% konnte nicht auf Viren geprüft werden, da er passwortgeschützt ist."

- Verschlüsselte E-Mails werden nicht gescannt, sondern ungeschannt zugestellt.
- Bezüglich der maximalen Länge von E-Mail Betreffzeilen und der maximalen Länge von Namen von Anhängen in einer E-Mail hält sich Dataport an den RFC Standard. Nicht diesem Standard entsprechende E-Mails werden abgewiesen.
- Verteilerlisten der Mailingorganisation @wibes.de sind von extern nicht anschreibbar.
- Innerhalb der Mailingorganisation @wibes.de gelten die **Outlook-Security Settings**.

7 Postfix

Der Postfix fungiert als annehmender E-Mail Server, welcher die von extern kommenden E-Mails an @wibes.de weiter versendet. Folgende Prüfungen finden auf dem Postfix statt:

- E-Mail – Empfängerprüfung. Es werden nur E-Mails für Empfänger angenommen, die in WiBeS Exchange bekannt sind. Hierfür wird einmal täglich (nachts) eine Whitelist aus dem WiBeS-AD mit allen E-Mail Adressen generiert und auf dem Postfix hinterlegt.
Hinweis: Wird ein Postfach neu angelegt, ist es somit erst am nächsten Tag von extern erreichbar. Dies gilt auch für neu gesetzte Alias-Adressen oder veränderte E-Mail Adressen (z.B. Namensänderung durch Hochzeit).
- E-Mails von extern, die mit einer internen WiBeS E-Mail Adresse als Absender kommen, werden an den Absender zurückgewiesen.
- Auf dem Postfix wird "Greylisting" durchgeführt. Greylisting bezeichnet eine Form der Spam-Bekämpfung bei E-Mails die von extern kommen - dabei wird die erste E-Mail von unbekanntem Absender zunächst abgewiesen und erst nach einem weiteren Zustellversuch angenommen.
- Eine Mailannahme auf dem Postfix erfolgt nur von bekannten, im Internet veröffentlichten festen IP-Adressen der entsprechenden Internet Service Provider. E-Mails aus IP Bereichen, die dynamischen IP-Adressen zugeordnet sind, werden abgewiesen.

Der Postfix leitet die E-Mails dann an die Virenschann-Server weiter – siehe nachfolgenden Punkt 8.

8 E-Mail Virenschutz (von und nach extern)

Alle eingehenden und ausgehenden E-Mails werden grundsätzlich nach Viren gescannt.

Von den Anti-Virenservern nicht scannbare E-Mails landen in der Quarantäne. Der Empfänger der E-Mail erhält hierüber eine Informations – E-Mail. Die Quarantäne kann nur vom Dataport Exchange Administrator eingesehen und aufgehoben werden. Hierfür schickt der User an die Exchange Administration von Dataport eine E-Mail.

Es können bei Bedarf zusätzliche Policies durch den Dataport Exchange Administrator eingerichtet werden. Aufträge hierfür sind von der Fachlichen Leitstelle an das Postfach wibes@dataport.de zu richten.

Dataport ist durch die Dataport Exchange Administration berechtigt, auf den Anti-Virenservern zusätzliche Policies zur Gefahrenabwehr eigenständig und ohne Rücksprache mit der Fachlichen Leitstelle einzurichten. Gegenüber der Fachlichen Leitstelle hat Dataport nur eine Informationspflicht. Weitere Pflichten ergeben sich daraus nicht.

Verschlüsselte E-Mails werden nicht gescannt und nicht aufgehoben.

Passwortgeschützte ZIP – Files werden nicht gescannt und nicht aufgehoben, lediglich mit einem Eintrag versehen:

"Der Anhang %FILENAME% konnte nicht auf Viren geprüft werden, da er passwortgeschützt ist."

8.1 Von extern

Alle **von extern** eingehenden E-Mails nach wibes.de werden nach Viren / Spyware / Greyware überprüft. Sollten Viren / Spyware / Greyware gefunden werden, wird versucht die E-Mail / den Anhang zu säubern. Gelingt dies nicht, wird der Anhang gelöscht.

Dann wird die E-Mail mit folgendem Eintrag versehen:

"Es wurde eine potentiell gefaehrliche Anlage %FILENAME% aus dieser Mail entfernt."

Alle **von extern** eingehenden E-Mails nach @wibes.de werden nach folgende ausführbaren Dateien durchsucht:

- Executable
- COM
- EXE
- DLL
- Java byte code (.js, .jse, .cla. and .class)
- Self-extracting compressed files (.lzh)

Werden ausführbare Dateien gefunden, werden diese gelöscht.

Die E-Mail wird mit folgendem Eintrag versehen:

"Es wurde eine potentiell gefaehrliche Anlage %FILENAME% aus dieser Mail entfernt."

Weiterhin finden folgende Prüfungen statt:

Gesamt E-Mail Größe:	10 MB
Maximale Empfängerzahl in einer E-Mail:	1000 Empfänger
Maximal eingebettete Ebenen in komprimierten Anhängen:	5 Ebenen
Maximal dekomprimierte Filegröße:	50 MB (Minimum 1 MB)
Maximale Anzahl von Files in einem komprimierten File:	1000 Files

Wird gegen eine dieser Limitierungen verstoßen, wird die E-Mail in Quarantäne verschoben und der Empfänger der E-Mail bekommt folgende Mitteilung:

"Die Viruswall konnte diese Mail nicht zustellen, da sie gegen interne Sicherheitseinstellungen verstößt. Bitte melden Sie sich gegebenenfalls beim CCF, um weitere Details zu erfahren."

Der Virenschann-Server leitet die E-Mail dann an den Anti-Spam Server weiter – siehe Punkt 9.

8.2 Nach Extern

Alle von wibes.de **nach extern** ausgehenden E-Mails werden nach Viren / Spyware / Greyware überprüft. Sollten Viren / Spyware / Greyware gefunden werden, wird versucht die E-Mail bzw. den Anhang zu säubern. Gelingt dies nicht, wird der Anhang gelöscht. Dann wird die E-Mail zugestellt, aber mit folgendem Eintrag versehen:

"Es wurde eine potentiell gefaehrliche Anlage %FILENAME% aus dieser Mail entfernt."

9 E-Mail Spamschutz

Alle an @wibes.de eingehenden E-Mails werden grundsätzlich nach Spam / Phishing gescannt.

9.1 Von extern

Wird eine E-Mail als Spam / Phishing erkannt, wird diese in die zentrale Quarantäne verschoben. Die E-Mails verbleiben dort für 50 Tage in der Quarantäne und werden erst dann automatisch gelöscht. Der Absender und der Empfänger der als Spam / Phishing erkannten E-Mail werden über das Abfangen der E-Mail nicht informiert. Die Dataport Exchange Administratoren können E-Mails innerhalb der 50 Tage Frist aus der Spam Quarantäne freigeben.

Aufträge hierfür sind von der Fachlichen Leitstelle an das Postfach wibes@dataport.de zu richten.

Es können bei Bedarf zusätzliche Policies durch den Dataport Exchange Administrator eingerichtet werden. Aufträge hierfür sind von der Fachlichen Leitstelle an das Postfach wibes@dataport.de zu richten.

Dataport ist durch die Exchange Administration berechtigt, auf dem Anti-Spam Server zusätzliche Policies zur Gefahrenabwehr eigenständig und ohne Rücksprache mit der Fachlichen Leitstelle einzurichten. Gegenüber der Fachlichen Leitstelle hat Dataport nur eine Informationspflicht. Weitere Pflichten ergeben sich daraus nicht.

9.2 Nach Extern

Eine Überprüfung der E-Mails nach Spam, die von @wibes.de nach extern geschickt werden, findet nicht statt.

10 E-Mail Virenschutz (intern)

Alle innerhalb der WiBeS Organisation versandten E-Mails werden ebenfalls auf Viren gescannt. Sollte ein Virus gefunden werden, wird versucht, die E-Mail bzw. den Anhang zu säubern. Gelingt dies nicht, wird der Anhang gelöscht. Dann wird die E-Mail zugestellt, aber mit folgendem Eintrag versehen:

"Es wurde eine potentiell gefaehrliche Anlage %FILENAME% aus dieser Mail entfernt."

11 Leistungsabgrenzung

Die zur Nutzung des E-Mail Dienstes notwendigen Software-Komponenten auf den Endgeräten der Nutzer sind nicht Gegenstand dieser LB. Die notwendigen Lizenzen auf den Clients zur Nutzung der Funktionen sind ebenfalls nicht Gegenstand dieser LB.

Service Level Agreement

Bereitstellung der Infrastruktur und Betrieb des Verfahrens WiBeS im Rechenzentrum

Allgemeiner Teil (Teil A)

für

Auftraggeber: Behörde für Schule und Berufsausbildung (BSB)

Straße: Hamburger Straße 31

Ort: 22083 Hamburg

nachfolgend Auftraggeber

Version: 2.1
Stand: 14.06.2013

Inhaltsverzeichnis

1	Einleitung	4
1.1	Aufbau des Dokumentes.....	4
1.2	Leistungsgegenstand.....	4
2	Rahmenbedingungen	5
2.1	Beschreibung des Fachverfahrens	5
2.2	Changemanagement.....	5
2.2.1	Changes mit vorab gegebener Zustimmung.....	5
2.2.2	Changes mit Zustimmung des Auftraggebers	6
2.2.3	Freigabe	6
2.3	Mitwirkungsrechte und –pflichten.....	6
2.4	Kündigungsmodalitäten	7
3	Leistungsbeschreibung	8
3.1	Infrastruktur	8
3.1.1	Rechenzentrum.....	8
3.1.2	Netzwerk-Anbindung und Firewall	9
3.1.3	Serverbasierte Leistungen Windows und Unix	9
3.1.4	Technisches Design.....	10
3.2	Bereitstellung	10
3.2.1	Systeme im Rechenzentrum.....	10
3.2.2	Systeme in den Räumlichkeiten des Auftraggebers	10
3.3	Betrieb und Administration.....	11
3.3.1	Basisbetrieb	11
3.3.2	Backup & Recovery.....	11
3.3.3	User – Administration.....	11
3.3.4	Datenbank und Middleware Administration	12
3.3.5	Applikations-Betrieb und Administration	12
3.3.6	Batch-Betrieb	12
3.3.7	Erneuerung und Ergänzung.....	13
3.3.8	Wartung und Pflege	13
3.3.9	Fernzugriff und Fernwartung, Fernunterstützung und Fernbedienung.....	14
3.3.10	Kommunikationsanbindung zum RZ.....	14
4	Leistungskennzahlen	16
4.1	Definition	16

4.1.1	Begriffsfestlegungen	16
4.2	Leistungsausprägung	16
4.3	Vereinbarte Leistungskennzahlen	17
4.4	Reporting	18
5	Erläuterungen	19
5.1	Erläuterung VDBI	19

1 Einleitung

Der Auftragnehmer stellt dem Auftraggeber IT Ressourcen einschließlich Hardware und systemnaher Software sowie IT Dienstleistungen mit dem vereinbarten Leistungsumfang bedarfsgerecht zur Verfügung (im Folgenden als Verfahren bezeichnet). Mit dieser Leistungsvereinbarung (Service Level Agreement, SLA) wird der Leistungsgegenstand geregelt. Darüber hinaus beschreibt das Dokument die Systemumgebung, die Aufgaben und Zuständigkeiten vom Auftragnehmer und vom Auftraggeber, sowie die vereinbarten Leistungskennzahlen (Service Levels).

1.1 Aufbau des Dokumentes

Diese Anlage enthält die folgenden Kapitel:

Rahmenbedingungen (Kapitel 2): Regelung von allgemeinen Rechten und Pflichten von Auftraggeber und Dienstleister, Bestimmungen zur Laufzeit, Änderung bzw. Kündigung der Vereinbarung sowie Übergangsbestimmungen.

Leistungsbeschreibungen (Kapitel 3): Inhaltliche Beschreibung der bereitgestellten Rechenzentrumsleistungen sowie der für einen reibungslosen Betrieb erforderlichen Dienstleistungen. Bestandteil der Leistungsbeschreibungen ist die in diesem Dokument beschriebene Verteilung von Aufgaben und Zuständigkeiten zwischen Auftraggeber und Dienstleister (VDBI – Erläuterungen s. Pkt. 5.1).

Leistungskennzahlen (Kapitel 4): Definition von Leistungskennzahlen und ihrer Messverfahren (z. B. Verfügbarkeit oder Reaktionszeiten), Festlegung von Betriebs- und Servicezeiten und Vereinbarungen über die zu erreichende Leistungsqualität (Service Level Objectives).

Erläuterungen (Kapitel 5)

1.2 Leistungsgegenstand

Gegenstand dieses Service Level Agreements ist die Bereitstellung der Dienstleistungen im Rechenzentrum.

Die allgemeinen Leistungen werden hinsichtlich der Leistungsqualität und des Leistungsumfangs im Kapitel 3 beschrieben. Die verfahrensspezifischen Leistungen werden im Teil B beschrieben.

2 Rahmenbedingungen

2.1 Beschreibung des Fachverfahrens

Die Beschreibung des Fachverfahrens und der zu Grunde liegenden Lösung erfolgt im Teil B.

2.2 Changemanagement

Das Changemanagement erfolgt in einem geregelten Prozess. Es ist die Aufgabe des Changemanagements sicherzustellen, dass standardisierte Vorgehensweisen zur Durchführung von Veränderungen existieren und effizient genutzt werden.

Der Auftragnehmer erbringt folgende Leistungen im Rahmen des Changemanagements für den Rechenzentrumsbetrieb.

2.2.1 Changes mit vorab gegebener Zustimmung

Der Auftraggeber stimmt mit Abschluss dieses Vertrages allen Änderungen an der Hardware, am Betriebssystem oder in den systemnahen Diensten, die die Integrität oder Verfügbarkeit des Verfahrens- oder des Services nicht berühren zu.

Aufgaben und Zuständigkeiten	Auftrag- nehmer	Auftrag- geber
Prüfung des Änderungsbedarfs	V, D	I, B
Durchführung in einer Testumgebung einschließlich der Dokumentation, wenn im Leistungsumfang enthalten.	V, D	I, B
Umsetzung der in der Testumgebung getesteten Änderungen in der Produktionsumgebung im vertraglich festgelegten Wartungsfenster und Ergänzung der Systemdokumentation	V, D	I, B
Anpassung der Verfahrensdokumentation, soweit dies durch eine Änderung erforderlich wird	V, D	I, B

2.2.2 Changes mit Zustimmung des Auftraggebers

Der Auftragnehmer holt für alle Änderungen, die die Integrität oder Verfügbarkeit des Verfahrens- oder des Services berühren die jeweilige Zustimmung des Auftraggebers ein. Dies gilt auch für Änderungen an den Verfahren und Services selbst.

Aufgaben und Zuständigkeiten	Auftragnehmer	Auftraggeber
Ermittlung des Änderungsbedarfs durch den Auftragnehmer oder Beauftragung durch den Auftraggeber.	V, D	V, D
Bei Ermittlung des Änderungsbedarfs durch den Auftragnehmer wird dem Auftraggeber oder seinen Beauftragten ein Änderungsantrag schriftlich oder per E-Mail zur Zustimmung übermittelt.	V, D	I, B
Durchführung von genehmigten Änderungen in einer Testumgebung (sofern beauftragt) einschließlich der Dokumentation des Auftraggebers unter Berücksichtigung der in Beauftragung enthaltenen Dringlichkeitsangabe.	V, D	I, B
Mitteilung der Testergebnisse (Testdokumentation und Stellungnahme) an den Auftraggeber oder seinen Beauftragten.	V, D	I, B
Der Auftraggeber führt den Test in der Testumgebung (sofern beauftragt) durch und beauftragt die Umsetzung der Änderungen in der Produktionsumgebung schriftlich oder per E-Mail.	I, B	V, D
Abstimmung des Umsetzungszeitpunktes und ggf. notwendigen Wartungsfensters mit dem Auftraggeber oder seinen Beauftragten.	V, D	I, B
Durchführung der Änderungen in der Produktionsumgebung und Ergänzung der Systemdokumentation.	V, D	I, B
Der Auftraggeber führt Tests in der Produktionsumgebung durch und erklärt die Freigabe der Änderungen in der Produktionsumgebung schriftlich in Papierform oder in Textform (Fax, E-Mail, etc.).	I, B	V, D
Anpassung der Verfahrensdokumentation, soweit dies durch eine Änderung erforderlich wird.	V, D	I, B

2.2.3 Freigabe

Mit der Freigabe des bezeichneten Freigabegegenstandes wird vereinbart, dass das System in der existierenden Form genutzt werden soll. Für Test und Freigabe von Verfahren ist der Auftraggeber verantwortlich. Automatisierte Verfahren, die der Auftragnehmer in eigener Verantwortung betreibt, werden vor ihrem erstmaligen Einsatz oder nach Änderungen getestet und freigegeben.

Die Freigabe von Test-, Schulungs- oder Produktivsystemen kann sowohl in Papier- als auch in Textform (Fax, E-Mail, etc.) erfolgen. Im Falle von umfangreicheren Systemen kann ein Freigabeprotokoll neben dem reinen Einverständnis zudem z.B. folgende Parameter festhalten:

- Konfigurationsstände
- Zusammenstellung und Bezeichnung der Datenbanken
- Benutzerhandbücher, technische Dokumentation

2.3 Mitwirkungsrechte und -pflichten

Die vom Auftragnehmer zugesagten Leistungen erfolgen auf Anforderung des Auftraggebers. Es sind Mitwirkungs- und Bereitstellungsleistungen des Auftraggebers erforderlich, die grundsätzlich in einer besonderen Anlage geregelt sind.

2.4 Kündigungsmodalitäten

Bei Beendigung der Vertragsbeziehung sind vom Auftragnehmer innerhalb von 6 Wochen nach Zustellung der Kündigung dem Auftraggeber die Unterlagen zur Verfügung zu stellen, die erforderlich sind, um den Geschäftsbetrieb unter geänderten Bedingungen fortzusetzen.

Dazu gehören unter anderem:

- Eine aktuelle Darstellung der im Zusammenhang mit diesem Vertrag genutzten Hardware.
- Eine aktuelle Aufstellung der für den Systembetrieb installierten Software.
- Die Übergabe der Lizenzunterlagen, soweit der Auftraggeber Lizenznehmer ist.
- Eine aktuelle Version der eingesetzten Standardkonfigurationen.
- Eine Dokumentation des eingesetzten Datensicherungssystems.
- Ein Exemplar einer aktuellen Datensicherung bzw. eines Datenexportes.
- Die Dokumentation der zu dem Zeitpunkt offenen Problemmeldungen und Aufträge.
- Jeweils eine Kopie der dem AG zuzuordnenden Handbücher, Hand-Outs und Dokumentationen.

Am Ende des letzten Tages des Vertrages bzw. der tatsächlichen Nutzung der Systeme sind vom Auftragnehmer an den Auftraggeber zu übergeben:

- der aktuelle Datenbestand,
- der Bestand der gesicherten Daten,
- alle dem Auftraggeber zuzuordnenden mobilen Datenträger (z. B. Installations-CDs, Sicherungsbänder)

Der Auftragnehmer wirkt auf Wunsch des Auftraggebers an einer durch Vertragsende durchzuführenden Migration mit. Aufwand, der durch eine solche Migration beim Auftragnehmer entsteht, sowie Materialaufwendungen und Aufwandsleistungen für individuelle Abschluss- und Sicherungsarbeiten werden vom Auftraggeber gesondert vergütet.

Der Auftragnehmer verpflichtet sich mit dem Vertragsende alle aus diesem Vertrag bezogenen Dateien und Programme in seiner Systemumgebung zu löschen.

3 Leistungsbeschreibung

Für den Betrieb des Verfahrens werden die im Teil B beschriebenen IT-Services durch den Auftragnehmer erbracht. Dies beinhaltet die anteilige Nutzung der erforderlichen Systemkonfiguration (Host, Server, Betriebssystem, betriebssystemnahe Software, Platten etc.) und alle notwendigen Services zur Sicherstellung eines reibungslosen Betriebs.

3.1 Infrastruktur

Die Leistung des Auftragnehmers erfolgt ausschließlich auf unterstützten Plattformen, die durch Hersteller freigegebenen sind. Daraus ergibt sich regelmäßig eine Veränderung der Infrastruktur / Plattform. Um den laufenden Betrieb zu sichern, werden diese Veränderungen für den zentralen Teil nach Maßgabe des Auftragnehmers realisiert. Dies wird im Rahmen der Regelkündigungsfristen angekündigt. Der Auftraggeber ist verpflichtet, die in seinem Auftrag gehosteten Verfahren und Komponenten rechtzeitig an diese veränderten Anforderungen anzupassen.

3.1.1 Rechenzentrum

Der Auftragnehmer stellt für den Betrieb der Rechnersysteme, die Bestandteil dieses Vertrages sind, entsprechende Fläche und Infrastruktur in den Standorten des Rechenzentrums (RZ) zur Verfügung. Die RZ Infrastruktur weist folgende Charakteristika auf:

1. Aufstellung im Rechenzentrum des Auftragnehmers
2. Betrieb in gesicherter Rechenzentrumsumgebung mit Zutrittschutz und Zugangsschutz
3. Brandschutzmaßnahmen (für die Systemräume Feuerschutz- Isolierung, Brandmeldezentrale, Durchschaltung zur Feuerwehr, Löschvorrichtungen)
4. Zutrittskontrolle und Überwachung in allen Gebäudebereichen, Personenvereinzelungsanlage im Rechenzentrum, Einbruchmeldeanlage, Wachdienst (7x24) vor Ort
5. Redundante unterbrechungsfreie Stromversorgung, Notstrom und Klimatisierung
6. Bereitstellung der Server
7. Installation und Konfiguration der System-Software
8. Bereitstellung, Betrieb und Wartung der erforderlichen Server
9. Tägliche Datensicherung
10. Sachgerechte Lagerung der gesicherten Daten (Datensicherung, Diebstahl- u. Brandschutz)
11. Rücksichern / Wiederherstellen von Daten/Datenbank im Schadensfall
12. Nutzung zentraler Sicherungsinfrastruktur, Magnetbandarchiv
13. Bereitstellung und Verwalten von Speichermedien
14. System- und Applikationsmonitoring mit aktiver Prozessüberwachung
15. Problemanalyse und Störungsbearbeitung
16. Einbindung der Infrastruktur in das LAN/WAN, Firewall
17. Automatische Überwachung über Netzwerk-Management
18. Patchmanagement
19. Virenschutz

3.1.2 Netzwerk-Anbindung und Firewall

Bestandteil der Leistung ist die Anbindung der für die Leistungserbringung erforderlichen Komponenten an das LAN des Rechenzentrums bis zum Übergabepunkt des WAN- bzw. Internet Providers.

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Spezifikation der für die Netzwerkkommunikation erforderlichen Protokolle und Kommunikations-Ports (Kommunikations-Matrix)	B, I	V, D
Beauftragung und Umsetzung der Netzwerkfreeschaltungen für Netzverbindungen, die in der Verantwortung des Auftragnehmers liegen	V, D	I
Beauftragung von Netzwerkfreeschaltungen für Netzverbindungen, die nicht in der Verantwortung des Auftragnehmers liegen	B, I	V, D

3.1.3 Serverbasierte Leistungen Windows und Unix

Der Auftragnehmer stellt für die im Teil B spezifizierten Services zugesicherte Ressourcen bereit. Zugesicherte Ressourcen werden durch Leistungsparameter beschrieben.

Es werden zwei verschiedene Konfigurationen der Plattform unterschieden (gilt auch für virtuelle Systeme):

- **Fest zugewiesene Systemressourcen:** Dem Auftraggeber stehen die Systemressourcen zur ausschließlichen Nutzung zur Verfügung. Die Dimensionierung muss dabei den geplanten Spitzen-Belastungen entsprechen. Die Konfiguration und Ressourcen der einzelnen Systeme sind im Anhang angegeben und stehen dem Auftraggeber exklusiv zur Verfügung.
- **Gemeinsam genutzte Systemressourcen:** Hardware und ggf. Software wird von mehreren Auftraggebern genutzt. Für den Spitzenlastausgleich können die Lastprofile aller beteiligten Auftraggeber ganzheitlich betrachtet werden.

Zugesicherte Ressourcen für Windows und UNIX

Die Leistungsbeschreibung beschreibt die jeweils bereitgestellten zugesicherten Ressourcen auf Basis normalisierter Leistungseinheiten.

Leistungseinheiten zu zugesicherten Serverleistungen

- Höhe der zugesicherten Leistung (CPU-Kerne)
- Zugesicherter RAM Hauptspeicher
- Zugesicherte Speicherleistung (für Daten und Programme)

Leistungseinheiten zu zugesicherten Datenbankleistungen

- Höhe der zugesicherten Leistungen (CPU-Kerne)
- Zugesicherter Hauptspeicher
- Anzahl Instanzen
- Anzahl Datenbanken
- Zugesicherte Speicherleistung (für die Datenbanken)

Leistungseinheiten zu zugesicherten Speicherleistungen

- Bereitgestellte Speicherleistung in GB pro Jahr

3.1.4 Technisches Design

Der Auftragnehmer entwickelt eine technische Architektur und stimmt diese mit den Anforderungen des Auftraggebers ab.

Die einzelnen Aufgaben und die Verteilung der Zuständigkeiten sind wie folgt geregelt:

Aufgaben und Zuständigkeiten	Auftragnehmer	Auftraggeber
Informationsbereitstellung von relevanten Normen, Anwendungsarchitekturen und Projektinitiativen	I, B	V, D
Abstimmung der applikationsrelevanten Teile des Technologieplans mit dem Auftraggeber (initial und bei erforderlicher Änderung)	V, D	I

3.2 Bereitstellung

Bereitstellung umfasst alle Maßnahmen im Zusammenhang mit der Installation neuer oder erneuerter Hardware- bzw. Systemsoftware-Komponenten.

Die einzelnen Aufgaben und die Verteilung der Zuständigkeiten sind wie folgt geregelt:

3.2.1 Systeme im Rechenzentrum

Aufgaben und Zuständigkeiten	Auftragnehmer	Auftraggeber
Erweiterungen der technischen Infrastruktur	V, D, B	I
Bereitstellung der neuen / zusätzlichen Ressourcen (Server, Platten etc.) gemäß Teil B	V, D	I
Installation und Konfiguration von Hardware, Betriebssystem und betriebssystem naher Software (z.B. Middleware) inkl. Einrichtung notwendiger User-Profile und Zugriffsmechanismen, Installation von Komponenten zur Überwachung und Steuerung des Systems und für die Ausgestaltung des Backup	V, D	I
Durchführung der Datenmigration im Zusammenhang dem Austausch von Systemkomponenten. Ausgenommen sind Datenmigrationen in Folge einer Neuimplementierung oder Plattformmigration.	V, D	I
Durchführung geeigneter Tests bei allen Installationen, Umzügen, Erweiterungen, Veränderungen der systemtechnischen Infrastruktur	V, D	I

3.2.2 Systeme in den Räumlichkeiten des Auftraggebers

Die Aufstellung von Systemen in den Räumlichkeiten des Auftraggebers ist möglich. Die inhaltliche Ausgestaltung kann dem Teil B entnommen werden.

3.3 Betrieb und Administration

Leistungen für Betrieb und Administration sind alle Maßnahmen, die im Zusammenhang mit der laufenden Verwaltung installierter Systeme und Softwareumgebungen (Betriebssystem, systemnahe Software) erbracht werden, um einen reibungslosen Betrieb sicherzustellen. Darunter fallen auch die Aufgaben zum Backup & Recovery. Die Aufgaben und Zuständigkeiten sind nachfolgend geregelt.

3.3.1 Basisbetrieb

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Erstellung, Pflege und Bereitstellung Betriebshandbuch (BSI-Grundschrift)	V, D	B, I
Inhaltliche Abstimmung des Betriebshandbuchs mit dem Auftraggeber	V, D	B, I
Steuerung und Überwachung der Systeme. Proaktives Erkennen und Vermeiden von Störungen	V, D	I
Überwachung der einzelnen Komponenten auf wesentliche Kenngrößen wie CPU Auslastung, Performance, Speicherressourcen und Störanzeichen durch Einsatz entsprechender System Monitoring Tools.	V, D	I
Sammlung und Übermittlung von Kenngrößen für die Anfertigung von Berichten	V, D	I
Beseitigung von Störungen, Restart / Recovery von Systemkomponenten unter Einhaltung der Eskalationsverfahren	V, D	I
Antwort auf Anfragen zu Störungen und Problemen beim Kunden	V, D	I
Durchführung von Diagnoseprozeduren entsprechend der Betriebsanweisungen	V, D	I
Benennung möglicher Produktveränderungen zur Leistungsoptimierung oder Kostensenkung für den Auftraggeber	V, D	I
Durchführung und Koordination von Konfigurationsmanagement und Change Management für alle betriebsrelevanten Bereiche	V, D	I

3.3.2 Backup & Recovery

Abhängig von der gewählten SLA-Klasse wird eine Zuordnung der Aufgaben und Zuständigkeiten im Teil B beschrieben.

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Definition von Backup Anforderungen und Aufbewahrungszeiträumen	I	V, D
Definition von Backup mit Zeitplänen, Vorgehensweisen, Parametern	V, D	I
Implementierung der System- und Datenbanksicherung	V, D	B, I
Durchführung der Datensicherung von System- und Applikationsdaten entsprechend der festgelegten Verfahrensweise (dezentral mit Unterstützung des Auftraggebers)	V, D	I
Durchführung von Recovery Maßnahmen entsprechend der bestehenden Richtlinien	V, D	I

3.3.3 User – Administration

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Bereitstellung der Auftraggeber relevanten Informationen und Vorgehensweisen, die für das Berechtigungskonzept erforderlich sind	I, B	V, D
Definition von Richtlinien für Administration (Berechtigungskonzept)	V, D	I

Aufgaben und Zuständigkeiten	Auftragnehmer	Auftraggeber
Beauftragung von Berechtigungsänderungen mit Bereitstellung der im Rahmen des Berechtigungskonzeptes definierten administrativen Daten (z. B. Personalnummer, erforderliche Berechtigungsstufe) bei neuen, geänderten und ausscheidenden Benutzern.	D	V
Einrichten und Verwaltung von Zugriffsberechtigungen von Anwendern für die einzelnen Systeme	D	V
Anfertigung von Berichten zu administrativen Tätigkeiten nach Abstimmung (z. B. Statistik User neu, geändert, gesamt für verschiedene Systeme / Plattformen)	V, D	I, B

3.3.4 Datenbank und Middleware Administration

Aufgaben und Zuständigkeiten	Auftragnehmer	Auftraggeber
Bereitstellung der Vorgaben für das Anlegen, Upgrade und Refresh von Datenbanken und Middleware Komponenten	V, D	I
Bereitstellung aller erforderlichen Informationen und Quellen (Datenträger) zur Installation und Wiederherstellung der Datenbank- und Middlewarekomponenten	I, B	V, D
Erstinstallation, Upgrade und Refresh von Datenbanken und Middleware	V, D	I
Pflege von Betriebsdokumentationen	V, D	
Überwachung und Steuerung der Datenbank-Systeme, Transaktionsmonitore und Middleware-Komponenten	V, D	
Speicherplatzüberwachung der Datenbanken und Middleware	V, D	
Mitteilung bei erforderlichen Speicherplatzweiterungen mit finanziellen Auswirkungen an den Auftraggeber	V, D	I
Beseitigung von Störungen bei auftretenden Datenbankproblemen im Betrieb und Ergreifen von Gegenmaßnahmen im Störfall	V, D	B
Einleitung des vereinbarten Eskalationsprozesses	V, D	I
Einspielen von Patches	V, D	I
Wartung der Datenbank	V, D	

3.3.5 Applikations-Betrieb und Administration

Grundsätzlich liegt das technische Verfahrensmanagement beim Auftragnehmer. Das technische Verfahrensmanagement beinhaltet die systemtechnische Installation, die Konfiguration und das Patchmanagement des Verfahrens, gemäß der vom Auftraggeber (oder von ihm beauftragten Dritten) vorgegebenen und bereitgestellten Installationspakete und Anweisungen (z. B. Ausführung von Setupprogrammen und Konfigurationen nach Checklisten).

- Das Technische Verfahrensmanagement ist erfüllt, wenn die Fachanwendung und ggf. definierte Programmteile starten.
- Ggf. notwendige Vor-Ort-Einsätze des Software-Herstellers (z. B. wenn die oben genannten Voraussetzungen nicht erfüllt sind) werden vom Auftraggeber gesondert beauftragt. Die dabei entstehenden Aufwände trägt der Auftraggeber.
- Installationsleistungen im Rechenzentrum des Auftragnehmers durch Mitarbeiter von Fremdfirmen oder des Auftraggebers müssen von einem Mitarbeiter des Auftragnehmers begleitet werden. Die Begleitung durch einen Mitarbeiter des Auftragnehmers wird gesondert in Rechnung gestellt.

Weitere Leistungen für den Applikations-Betrieb und der Administration werden im Teil B beschrieben.

3.3.6 Batch-Betrieb

Sofern diese Leistungen anfallen, werde diese im Teil B beschrieben.

3.3.7 Erneuerung und Ergänzung

Technologische Erneuerungs- und Ergänzungsleistungen sind alle Maßnahmen im Zusammenhang mit der routinemäßigen Modernisierung der IT-Infrastruktur, mit deren Hilfe sichergestellt wird, dass alle Systemkomponenten auf dem aktuellen Stand der technischen Entwicklung für branchenübliche Technologieplattformen erhalten werden. Die einzelnen Aufgaben und die Verteilung der Zuständigkeiten sind wie folgt geregelt:

Aufgaben und Zuständigkeiten	Auftrag-nahmer	Auftrag-geber
Einführung von Richtlinien und Verfahrensweisen für Erneuerungen und Ergänzung einschließlich Vorgaben für Erneuerungszyklen für eingesetzte Hardware- und Softwarekomponenten	V, D	I, B
Zustimmung zu den erstellten Richtlinien für Erneuerung und Ergänzung	I, B	V, D
Ersatz/Nachrüstung von Hardware und Software unter Verwendung geeigneter neuer Technologien	V, D	I, B

3.3.8 Wartung und Pflege

Um sämtliche Hardware-Systeme und die eingesetzte Software zum Betrieb der Infrastruktur im Rechenzentrum in einem – auch vom Hersteller unterstützten – Zustand zu halten, führt der Auftragnehmer kontinuierlich Verbesserungen und Änderungen durch. Dazu gehören:

Wartungsarbeiten:

Diese dienen der Erhaltung der Betriebsfähigkeit der eingesetzten Hardware. Der Auftragnehmer betreibt grundsätzlich Systeme, deren Komponenten (Betriebssystem, Datenbanken, etc) beim Hersteller unter Wartung sind.

Softwarepflege:

Die Softwarepflege dient der Verbesserung eines Softwareproduktes in Bezug auf die Funktionalität und Performance (*Release*) oder auf Grund von Fehlerbehebung (*Patch*).

Arbeiten, die im Rahmen der Wartung oder Softwarepflege vom Auftragnehmer erbracht werden, führt der Auftragnehmer innerhalb der normalen Büroarbeitszeiten bzw. innerhalb der vereinbarten Wartungszeitfenster durch. Dies gilt für Eingriffe, die die Nutzung des Service nicht übermäßig beeinträchtigen. Der Auftragnehmer entscheidet eigenständig über den Einsatz von Releases oder Patches, die vom Hersteller angeboten werden.

Arbeiten in der RZ-Umgebung, die mit Einschränkungen für den Auftraggeber verbunden sind, werden in den vereinbarten Wartungszeitfenstern vorgenommen und mit dem Auftraggeber abgestimmt.

Widerspricht der Auftraggeber einer vom Auftragnehmer empfohlenen Wartungsmaßnahme und entstehen dadurch Mehraufwände, so sind diese vom Auftraggeber zu tragen.

Die Verantwortlichkeiten für die einzelnen Wartungsaufgaben sind wie folgt geregelt:

Aufgaben und Zuständigkeiten	Auftrag-nahmer	Auftrag-geber
Definition von Richtlinien und Verfahrensweisen für Wartung und Reparatur, Einspielen von Patches und Releasewechsel	V, D	I
Prüfung der Relevanz von veröffentlichten Service Packs, Firmware, Patches etc.	V, D	I
Planung von systemspezifischen Wartungsarbeiten	V, D	I
Durchführung von exemplarischen Tests vor der Ausführung systemspezifischer Wartungsarbeiten	V, D	I

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Ausführung systemspezifischer Wartungsarbeiten (z. B. Installation von Service Packs, Firmware, Patches und Software Maintenance Releases)	V, D	I
Planung und Abstimmung von Releasewechseln mit dem Auftraggeber (insbesondere Applikationsexperten etc.)	V, D	B
Genehmigung von Releasewechseln hinsichtlich der Kompatibilität mit Systemen / Anwendungen, die unter Verantwortung des Auftraggebers betrieben werden.	V	B
Durchführung der Software-Distribution bei Release-wechsel; Versionskontrolle aller installierten Software Produkte einschließlich Anpassung der Schnittstellen der betroffenen Anwendungen, die vom Auftragnehmer betreut werden	V, D	I
Vorbeugende HW-Wartung entsprechend der Herstellerempfehlungen	V, D	I

3.3.9 Fernzugriff und Fernwartung, Fernunterstützung und Fernbedienung

Ein Fernzugriff liegt vor, wenn Mitarbeiter des Auftragnehmers oder beauftragte Dritte von einem System auf ein anderes System zu Wartungs-, Reparatur-, Bedienungs- oder Unterstützungszwecken, über nicht-dedizierte Kommunikationskanäle zugreifen.

„Fernzugriff“ ist der Oberbegriff für die im Folgenden dargestellten Fallarten:

- **Fernwartung**
Eine Fernwartung setzt eine administrative Tätigkeit von einem externen System auf ein internes System voraus.
Eine administrative Tätigkeit liegt vor, wenn die Tätigkeit der Verwaltung der Nutzbarmachung des IT-Fachverfahrens dient und nicht ausschließlich der Nutzung eines IT-Fachverfahrens oder dem Support aus Nutzersicht.
- **Fernunterstützung**
Die Fernunterstützung stellt einen „nur sehenden“ Fernzugriff, ohne direkte Kontrollmöglichkeit des Systems, dar.
- **Fernbedienung**
Mit Einverständnis des Nutzers kann die Fernunterstützung auch in Form einer Fernbedienung erfolgen. Der Zugreifende übernimmt die aktive Steuerung wahlweise mit dem Rechteprofil des Nutzers oder – nach dessen Abmeldung – mit einem auf dem Zielsystem hinterlegtem Fernbedienungs-Account.

Der Fernzugriff von Mitarbeiter des Auftragnehmers auf zu betreuende Systeme erfolgt in Übereinstimmung mit einem grundschutzkonformen Sicherheitskonzept am Maßstab eines hohen Schutzbedarfs.

Der Fernzugriff von beauftragten Dritten kann ausschließlich über eine vom Auftragnehmer vorgegebene Kommunikations-, Zugriff- und Infrastrukturlösung in Übereinstimmung mit einem grundschutzkonformen Sicherheitskonzept am Maßstab eines hohen Schutzbedarfs erfolgen.

Voraussetzung für die Einrichtung eines Fernzugriffs für Dritte ist der Nachweis, dass durch den Zugriff Dritter keine Gefahr für die Sicherheit der Daten und Ressourcen hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit entstehen.

Prüfung und Freigabe des Nachweises erfolgt durch den ITSB des Auftragnehmers.

Details zum Fernzugriff und zur Fernwartung, Fernunterstützung und Fernbedienung sind ggf. im Teil B geregelt.

3.3.10 Kommunikationsanbindung zum RZ



Der Auftraggeber gewährleistet, dass die Anwender des zentralen Verfahrens über einen Zugang zum Landesnetz oder einen mit dem Auftragnehmer abgestimmten, gleichwertigen Anschluss verfügen.

Der Auftraggeber stellt eine für den laufenden Betrieb ausreichend performante Netzanbindung sicher.

4 Leistungskennzahlen

4.1 Definition

Eine Leistungskennzahl ist eine Maßzahl, die zur Qualifizierung einer Leistung dient und der eine Vorschrift zur quantitativen reproduzierbaren Messung einer Größe oder Vorgangs zu Grunde liegt.

4.1.1 Begriffsfestlegungen

Betriebsmodus	Begriffsdefinition
Betriebszeit (unbetreuter Betrieb)	Die Betriebszeit ist der Zeitraum, in der die vereinbarten Ressourcen vom Auftragnehmer zur Verfügung gestellt und automatisiert überwacht werden.
Servicezeit	Servicezeiten beschreiben Zeiträume, in denen definierte Services zur Verfügung steht.
Supportzeit (betreuter Betrieb)	Die Servicezeit „Supportzeit (betreuter Betrieb)“ beschreibt die Zeiträume, in denen die Ressourcen vom Auftragnehmer bedient und Störungen und Anfragen bearbeitet werden.
Wartungsfenster	Regelmäßiges Zeitfenster für Wartungsarbeiten an den Systemen, in dem die Systeme nicht oder nur eingeschränkt für den Auftraggeber nutzbar sind. Sollte in Sonderfällen ein größeres oder weiteres Wartungsfenster beansprucht werden, so erfolgt dies in direkter Absprache mit dem Auftraggeber. Der Auftraggeber wird nur in begründeten Fällen die Durchführung von Wartungsmaßnahmen einschränken. Der Auftragnehmer wird in diesen Fällen unverzüglich über sich ggf. daraus ergebenden Mehraufwand und Folgen informieren.
Verfügbarkeit	Prozentualer Anteil an einer zugesagten Servicezeit (z. B. „Supportzeit betreuter Betrieb“) innerhalb eines Messzeitraumes, in der die beschriebenen Komponenten für den Auftraggeber nutzbar sind. $\text{Verfügbarkeit} = 1 - \frac{\sum \text{ungeplante Ausfallzeiten [h]}}{\text{Supportzeit (betreuter Betrieb) im Messzeitraum (Jahr) [h]}}$
Ausfallzeit	Die Ausfallzeit ist die Zeitspanne, die nach Eintritt der Nichtverfügbarkeit während der zugesagten Servicezeit vergeht, bis ein System (bzw. Systemcluster) mit allen Komponenten wieder für den Regelbetrieb zur Verfügung steht. Gemessen wird die Ausfallzeit in Stunden innerhalb der vereinbarten Servicezeiten.
Reaktionszeit	Die Reaktionszeit ist die Zeitspanne innerhalb der vereinbarten Servicezeiten zwischen der Feststellung einer Störung durch den Dienstleister bzw. Meldung einer Störung durch den Auftraggeber über den vereinbarten Weg (Service Desk) bis zum Beginn der Störungsbeseitigung. Die Reaktionszeit beginnt mit der Aufnahme der Störung in das Ticketsystem des Auftragnehmers.
Messzeitraum	Der Zeitraum, auf den sich eine Leistungskennzahl bezieht und in dem die tatsächlich erbrachte Qualität der Leistung gemessen wird. Sofern nicht anders angegeben beziehen sich alle angegebenen Metriken jeweils auf einen Messzeitraum von einem Kalenderjahr.

4.2 Leistungsausprägung

Die beschriebenen Leistungen sind jeweils in verschiedenen Ausprägungen mit unterschiedlichen Qualitätskriterien und Preisen verfügbar, um entsprechend den Anforderungen auf Kundenseite eine optimale Anpassung zwischen benötigter Leistung und Preis erreichen zu können.

Für Anwendungen mit nicht definiertem oder verbindlich abgeschlossenem Servicelevel wird zunächst die Leistungsausprägung **Typ 3 Standard** festgelegt.

Leistungsausprägung	Einsatzgebiet
Typ 1 (Höchstverfügbar) Premium Plus Premium Plus	Höchste Anforderungen bezüglich Verfügbarkeit und Priorität bei der Bereitstellung, Wartung und Störungsbeseitigung für den Betrieb besonders geschäftskritischer Systeme.
Typ 2 (Hochverfügbar) Premium	Hohe Anforderungen bezüglich Verfügbarkeit und Priorität bei der Bereitstellung, Wartung und Störungsbeseitigung für den Betrieb von geschäftskritischen Systemen.
Typ 3 (normale Verfügbarkeit) Standard	Durchschnittliche Anforderungen bezüglich Verfügbarkeit und mittlere Priorität bei der Bereitstellung, Wartung und Störungsbeseitigung für den Produktivbetrieb von Systemen, die nicht geschäftskritisch sind.
Typ 4 (einfache Verfügbarkeit) Economy	Niedrige Anforderungen bezüglich Verfügbarkeit und Priorität bei Bereitstellung, Wartung und Störungsbeseitigung für sonstige Systeme

Die Feststellung der Anforderungen an die Verfügbarkeit eines Systems und die Eingruppierung in eine Typklasse erfolgt vom Auftragnehmer gemeinsam mit dem Auftraggeber und wird im Teil B festgeschrieben.

4.3 Vereinbarte Leistungskennzahlen

Leistungskennzahlen für Betriebsleistungen.

SLA Klassen	1 Premium Plus	2 Premium	3 Standard	4 Economy
Betriebszeit (unbetreuter Betrieb)	7 Tage x 24 Stunden			
Supportzeit (betreuter Betrieb)	Mo-Do 08:00 - 17:00 Uhr Fr 8.00 – 15.00 Uhr			
Wartungsfenster	Di. 19:00 – Mi. 06:00 Uhr; Ausnahmen nach Vereinbarung			
Reaktionszeit im Störfall	30 Minuten		60 Minuten	120 Minuten
Zielverfügbarkeit des definierten Services	99,5	98,0	95,0	90,0
Storage- Verfügbarkeitsklassen (Obligatorisch bei RDBMS- Service)	Premium	Premium	Standard	Standard

Die Verfügbarkeit wird für zentrale Anwendungen bis zur Datenübergabeschnittstelle ans WAN / Internet garantiert, für dezentrale Anwendungen gilt die Gewährleistung am Erbringungsort.

Ist die Verfügbarkeit durch folgende Gründe gestört, so gilt die Gewährleistung der Verfügbarkeit für diese Zeiten nicht:

- aufgrund von höherer Gewalt und Katastrophen
- Qualität der beigestellten Software
- Unterbrechung aufgrund von Vorgaben des Auftraggebers
- infolge Unterbleibens oder verzögerter Erfüllung von Mitwirkungspflichten durch den Auftraggeber

Verfügbarkeitsklassen	Beschreibung
Premium	Für die Verfügbarkeitsklasse Premium werden gespiegelte Speichersysteme eingesetzt. Solche Systeme sind in sich mehrfach redundant aufgebaut, um höchste Verfügbarkeit zu gewährleisten. Ein Ausfall einer Einzelkomponente betrifft damit nur einen sehr geringen Teil des Gesamtsystems. Der Großteil steht ohne Funktions- oder Performanceeinbußen weiter zur Verfügung. Durch entsprechende redundante Anbindung eines Serversystems wird, je nach Anforderung an die Verfügbarkeit, auch dieser Fehlerfall vollständig abgefangen. Die Speichersysteme stehen auch während Software-Upgrades, Erweiterungen oder Konfigurationsänderungen unterbrechungsfrei zur Verfügung. Die Speichersysteme der Verfügbarkeitsklasse Premium sind für die SLA-Klassen Premium Plus und Premium Voraussetzung. Es gibt sie in den Konfigurationen Schutzbedarf „Normal“ und Schutzbedarf „Hoch“.
Standard	Für die Verfügbarkeitsklasse Standard kommen ungespiegelte Speichersysteme zum Einsatz. Alle Komponenten dieser Systeme sind mindestens doppelt ausgelegt, um bei Ausfall einer Komponente den weiteren Betrieb sicherzustellen. Durch entsprechende redundante Anbindung eines Serversystems wird, je nach Anforderung an die Verfügbarkeit, auch dieser Fehlerfall vollständig abgefangen. Software-Upgrades und Erweiterungen haben i.d.R. keine Auswirkungen auf den Betrieb. Midrangesysteme können für die SLA-Klassen Standard und Economy eingesetzt werden. Es gibt sie in den Konfigurationen Schutzbedarf „Normal“ und Schutzbedarf „Hoch“.

4.4 Reporting

Über die Auswertungen bzgl. der Einhaltung der Service Level erbringt der Auftragnehmer einen monatlichen Nachweis über die erbrachten Leistungen.

Der Nachweis umfasst folgende Bereiche:

- Gegenüberstellung zwischen den Messwerten der erbrachten Leistungskennzahlen und den definierten Sollwerten (Service Level Performance)
- Trendbewertung für vereinbarte Systemen bzgl. Auslastung, Performance, Kapazität entsprechend der definierten Richtlinien und daraus abgeleiteten Handlungsempfehlungen

5 Erläuterungen

5.1 Erläuterung VDBI

V = Verantwortlich	„V“ bezeichnet denjenigen, der für den Gesamtprozess verantwortlich ist. „V“ ist dafür verantwortlich, dass „D“ die Umsetzung des Prozessschritts auch tatsächlich erfolgreich durchführt.
D = Durchführung	„D“ bezeichnet denjenigen, der für die technische Durchführung verantwortlich ist.
B = Beratung	„B“ bedeutet, dass die Partei zu konsultieren ist und z.B. Vorgaben für Umsetzungsparameter setzen oder Vorbehalte formulieren kann. „B“ bezeichnet somit ein Mitwirkungsrecht bzw. eine Mitwirkungspflicht.
I = Information	„I“ bedeutet, dass die Partei über die Durchführung und/oder die Ergebnisse des Prozessschritts zu informieren ist. „I“ ist rein passiv.

Service Level Agreement

Bereitstellung der Infrastruktur und Betrieb *des* Verfahrens WiBeS im Rechenzentrum

Verfahrensspezifischer Teil (Teil B)

für

Auftraggeber: Behörde für Schule und Berufsausbildung (BSB)

Straße: Hamburger Straße 31

Ort: 22083 Hamburg

nachfolgend Auftraggeber

Version: 1.0
Stand: 05.05.14

Inhaltsverzeichnis

1	Einleitung	3
1.1	Aufbau des Dokumentes.....	3
1.2	Leistungsgegenstand.....	3
1.3	Ergänzende Informationen/Abgrenzungen zum SLA Teil A Allgemeiner Teil.....	3
1.3.1	Ergänzende Informationen.....	3
1.3.2	Abgrenzungen.....	3
2	Rahmenbedingungen	5
2.1	Mitwirkungsrechte und -pflichten.....	5
3	Leistungsbeschreibung	6
3.1	Infrastrukturleistungen.....	6
3.1.1	Netzwerk-Anbindung und Firewall.....	6
3.1.2	Serverbasierte Leistungen Windows und UNIX.....	6
3.1.2.1	Applikations- und Webservice.....	6
3.1.3	Backup & Recovery.....	7
3.1.4	Leistungsabgrenzung.....	7
3.2	Lizenzleistungen.....	8
3.2.1	Lizenzleistungen aus Landesverträgen / Rahmenverträgen.....	8
4	Leistungskennzahlen	8
4.1	Leistungsausprägung.....	9
4.1.1	Betriebszeiten.....	9
4.1.1.1	Onlineverfügbarkeit.....	9
4.1.1.2	Servicezeit - Betreuter Betrieb.....	9
4.1.1.3	Servicezeit - Überwachter Betrieb.....	9
4.1.2	Wartungsarbeiten.....	9
4.1.3	Support.....	9
4.1.4	Störungsannahme.....	10
4.1.5	Incident-Management.....	10
5	Erläuterungen	12
5.1	Erläuterung VDBI.....	12

1 Einleitung

Der Auftragnehmer stellt dem Auftraggeber IT Ressourcen einschließlich Hardware und systemnaher Software sowie IT Dienstleistungen mit dem vereinbarten Leistungsumfang bedarfsgerecht zur Verfügung (im Folgenden als Verfahren bezeichnet). Mit dieser Leistungsvereinbarung (Service Level Agreement, SLA) wird der Leistungsgegenstand geregelt.

1.1 Aufbau des Dokumentes

Diese Anlage enthält die folgenden Kapitel:

Rahmenbedingungen (Kapitel 2): Individuelle Regelung von Rechten und Pflichten von Auftraggeber und Dienstleister, Bestimmungen zur Laufzeit, Änderung bzw. Kündigung der Vereinbarung sowie Übergangsbestimmungen.

Leistungsbeschreibungen (Kapitel 3): Individuelle inhaltliche Beschreibung der bereitgestellten Rechenzentrumsleistungen sowie individuelle Vereinbarungen von für einen reibungslosen Betrieb erforderlichen Dienstleistungen.

Leistungskennzahlen (Kapitel 4): Individuelle Definition von Leistungskennzahlen und ihrer Messverfahren (z. B. Verfügbarkeit oder Reaktionszeiten), Festlegung von Betriebs- und Servicezeiten und Vereinbarungen über die zu erreichende Leistungsqualität (Service Level Objectives).

Erläuterungen (Kapitel 5)

1.2 Leistungsgegenstand

Gegenstand dieses Service Level Agreements ist die Bereitstellung der Dienstleistungen im Rechenzentrum.

Die allgemeinen Leistungen werden hinsichtlich der Leistungsqualität und des Leistungsumfangs im Teil A beschrieben. Die verfahrensspezifischen Leistungen werden im Teil B beschrieben.

1.3 Ergänzende Informationen/Abgrenzungen zum SLA Teil A Allgemeiner Teil

1.3.1 Ergänzende Informationen

- Punkt 3.2.2: Eine Aufstellung in den Räumen des Auftraggebers erfordert immer eine gesonderte detaillierte Prüfung der Gegebenheiten vor Ort. Ggfs. sind Bereitstellungsleistungen des Auftraggebers erforderlich, die dann in Punkt 3 dieses SLAs geregelt werden.
- Punkt 3.3.1: Produktveränderungen zur Leistungsoptimierung oder Kostensenkung für den Auftraggeber werden unter Berücksichtigung der aktuell geltenden RZ Standards zwischen Produktverantwortlichem, Architektur und dem Auftraggeber abgestimmt

1.3.2 Abgrenzungen

Die hier im Folgenden aufgeführten in Teil A definierten Services können teilweise erst mit dem Umzug der hier betroffenen Fachverfahren und zugehörigen Services in die neuen Dataport Rechenzentren (RZ²) reportet werden. Der Umzug erfolgt im Rahmen der Transitionen des Projekts RZ².

- Punkt 3.3.1: Sammlung und Übermittlung von Kenngrößen für die Anfertigung von Berichten
- Punkt 3.3.1: „Erstellung und Abstimmung von Betriebsführungshandbüchern nach „BSI_Grundschatz“
- Punkt 3.3.3: „Anfertigung von Berichten zu administrativen Tätigkeiten nach Abstimmung (z. B. Statistik User neu, geändert, gesamt für verschiedene Systeme / Plattformen)“
- Punkt 3.3.7: „Einführung von Richtlinien und Verfahrensweisen für Erneuerungen und Ergänzung einschließlich Vorgaben für Erneuerungszyklen für eingesetzte Hardware- und Softwarekomponenten“
- Punkt 4.4: „Reporting“

2 Rahmenbedingungen

2.1 Mitwirkungsrechte und -pflichten

Die vom Auftragnehmer zugesagten Leistungen erfolgen auf Anforderung des Auftraggebers. Es sind Mitwirkungs- und Bereitstellungsleistungen des Auftraggebers erforderlich.

Ergibt sich aus der Unterlassung von Mitwirkungspflichten und Nichtbeistellung des Auftraggebers von festgelegten Informationen / Daten eine Auswirkung auf die Möglichkeit der Einhaltung der Service Level, entlastet dies den Auftragnehmer von der Einhaltung der vereinbarten Service Level ohne Einfluss auf die Leistungsvergütung für die bereitgestellten Ressourcen.

3 Leistungsbeschreibung

3.1 Infrastrukturleistungen

Für den Fall, dass sich die Anforderungen an die dezentrale Infrastruktur ändern, gehen die dadurch erforderlich werdenden Anpassungen zu Lasten des Auftraggebers. Er stellt sicher, dass seine dezentrale Infrastruktur den laufenden Betrieb ermöglicht.

3.1.1 Netzwerk-Anbindung und Firewall

Für Dienststellen der Verwaltung des Landes Schleswig-Holstein, der Freien und Hansestadt Hamburg und der Hansestadt Bremen wird ein Zugang zum jeweiligen Landesnetz vorausgesetzt.

3.1.2 Serverbasierte Leistungen Windows und UNIX

3.1.2.1 Applikations- und Webservice

Es werden zugesicherte Ressourcen für die nachfolgend spezifizierten Services bereitgestellt.

Applikationsservice				
Windows Server 2008 R2				
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	Applikation Standard Dedicated-XLProduktion SharePoint Webfrontend	16	32	600
1	Applikation Standard Dedicated-XLProduktion Index/ Applikationsserver	16	32	600
Ergänzungen / Bemerkungen				

des betreuten Betriebs (Punkt 4.1.1.2 dieses SLAs) umfasst.

3.1.3 Backup & Recovery

Die Datensicherung umfasst die Sicherung sämtlicher Daten, die zur Ausführung und für den Betrieb der Verfahren notwendig sind. Diese wird gemäß Anforderung des Auftraggebers eingerichtet.

Programm-Dateien, Konfigurations-Dateien und Nutzdaten-Dateien. Verfahrensdaten, die in der Registry abgelegt sind, gehören zu den Systemdaten, die durch die Systemsicherung entsprechend zu sichern sind. Die Systemsicherung wird vom Auftragnehmer standardmäßig eingerichtet.

Gemäß Standard im Dataport Rechenzentrum erfolgt für Applikations-, Web- und Terminalservices einmal wöchentlich eine Vollsicherung sowie eine tägliche inkrementelle Sicherung.

Für Datenbankservices wird einmal tägliche eine Vollsicherung durchgeführt, dazwischen erfolgt alle drei Stunden eine Logsicherung.

Die gesicherten Daten werden 30 Tage aufbewahrt.

Im Fehlerfall bzw. auf Anforderung des Auftraggebers erfolgt eine Wiederherstellung der Daten.

Entsprechend den Anforderungen des Auftraggebers kann von den Standard-Sicherungszyklen abgewichen werden. Dies ist im Einzelfall auch unter Berücksichtigung der technischen Möglichkeiten abzustimmen.

3.1.4 Leistungsabgrenzung

Für Backendverfahren deren Frontend Applikation im GovernmentGateway ablaufen findet der erweiterte Betrieb und Supportlevel des GovernmentGateway keine Anwendung. Soweit ein erweiterter Betrieb mit höherem Supportlevel gewünscht ist, ist eine gesonderte Beauftragung dieser Leistung erforderlich.

3.2 Lizenzleistungen

Die Lizenzleistungen sind zwischen Auftraggeber und Auftragnehmer wie nachfolgend beschrieben vereinbart.

Aufgaben und Zuständigkeiten	Auftragnehmer	Auftraggeber
Betriebssystemlizenzen inklusive Wartung, Assurance	V,D	
Lizenzen für zentrale RZ-Dienste wie Datensicherung, Systemmanagement, Netzwerküberwachung	V,D	
Virenschutz auf allen Systemen, die der Auftragnehmer als Bestandteil dieses SLAs bereitstellt	V,D	
Fachanwendung		V,D
Lizenzleistungen aus Landesverträgen des Auftraggebers		V, D

3.2.1 Lizenzleistungen aus Landesverträgen / Rahmenverträgen

Lizenzleistungen, die der Auftraggeber durch Vereinbarungen außerhalb der hier vorliegenden Leistungsvereinbarung nutzen kann (z. B. aus Landesverträgen, Rahmenverträgen etc.), sind im Rahmen dieser Leistungsvereinbarung eine **Beistellungsleistung des Auftraggebers**.

Erlischt deren Nutzbarkeit für den Auftraggeber, ist der Auftraggeber verpflichtet, eine im Sinne des Lizenzrechts des Lizenzgebers gleichwertige Lizenzleistung beizubringen oder beim Auftragnehmer eine im Sinne des Lizenzrechts des Lizenzgebers gleichwertige Lizenzleistung zu beauftragen.

Die nachfolgend stehenden Lizenzen werden im Rahmen dieser Leistungsvereinbarung als Beistellungsleistung des Auftraggebers vom Auftragnehmer genutzt:

Sharepoint	x		x	Gruppe: Inter-/Intranetservices
Fachverfahren	x		x	Gruppe: Inter-/Intranetservices

4 Leistungskennzahlen

4.1 Leistungsausprägung

4.1.1 Betriebszeiten

4.1.1.1 Onlineverfügbarkeit

Die zentrale Infrastruktur steht ganztägig zur Verfügung, d.h. an sieben Tagen in der Woche, 24 Stunden pro Tag – ausgenommen der unten angegebenen Einschränkungen (z.B. Wartungsfenster).

4.1.1.2 Servicezeit - Betreuter Betrieb¹

- Montag bis Donnerstag 08.00 Uhr bis 17.00 Uhr
- Freitag 08.00 Uhr bis 15.00 Uhr

In diesen Zeiten erfolgt die Überwachung und Betreuung der Systeme durch Administratoren des Auftragnehmers. Es stehen Ansprechpartner mit systemtechnischen Kenntnissen für den Betrieb und zur Störungsbehebung zur Verfügung. Im Problem- und Störfall wird das entsprechende Personal des Auftragnehmers über das Call-Center des Auftragnehmers informiert.

4.1.1.3 Servicezeit - Überwachter Betrieb

- alle Zeiten außerhalb des betreuten Betriebes

Auch außerhalb des betreuten Betriebes stehen die Systeme den Anwendern grundsätzlich zur Verfügung. Die Systeme werden automatisiert überwacht. Festgestellte Fehler werden automatisch in einem Trouble-Ticket-System hinterlegt. Ansprechpartner stehen während des überwachten Betriebes nicht zur Verfügung.

4.1.2 Wartungsarbeiten

Die regelmäßigen, periodisch wiederkehrenden Wartungs- und Installationsarbeiten erfolgen i. d. R. außerhalb der definierten Servicezeiten des betreuten Betriebes. Derzeit ist ein Wartungsfenster in der Zeit von Dienstag 19:00 Uhr bis Mittwoch 06:00 Uhr definiert. In dieser Zeit werden Wartungsarbeiten durchgeführt und das Arbeiten ist nur sehr eingeschränkt möglich. In Ausnahmefällen (z.B. wenn eine größere Installation erforderlich ist) werden diese Arbeiten nach vorheriger Ankündigung an einem Wochenende vorgenommen.

4.1.3 Support

Der Auftragnehmer übernimmt den Support für die vom Auftragnehmer angebotenen Leistungen. Der Auftragnehmer übernimmt keine verfahrensbezogenen fachlichen Supportleistungen. Ggf. notwendige Vor-Ort-Einsätze des Software-Herstellers für technische oder fachliche Supportleistungen werden vom Auftraggeber beauftragt und die entstehenden Aufwände trägt der Auftraggeber.

- Support für den Betrieb erfolgt durch die Annahme von Störungsmeldungen und die Einleitung der Behebung des zugrunde liegenden Problems.
- Support für Verfahren sowohl vom Auftragnehmer als auch von anderen Herstellern ist nicht Bestandteil der Leistung und kann optional beauftragt werden.

¹ Gilt nicht für gesetzliche Feiertage, sowie 24.12. und 31.12.

4.1.4 Störungsannahme²

Die Störungsannahme erfolgt grundsätzlich über das Call-Center/den Userhelpdesk des Auftragnehmers.

Im Rahmen der Störungsannahme werden grundsätzlich Melderdaten sowie die Störungsbeschreibung erfasst und ausschließlich für die Störungsbehebung gespeichert. Der Störungsabschluss wird dem meldenden Anwender bekannt gemacht.

4.1.5 Incident-Management

Betriebsstörungen werden als Incidents im zentralen Trouble Ticket System (TTS) aufgenommen. Jeder Incident und dessen Bearbeitungsverlauf werden im TTS dokumentiert. Aus dem TTS lässt sich die Zeit der Störungsbearbeitung von der Aufnahme bis zum Schließen des Tickets mit der Störungsbehebung bestimmen.

Generell unterbrechen die Zeiten außerhalb des betreuten Betriebes die Bearbeitungszeit. Ebenso wird die Störungsbearbeitung unterbrochen durch höhere Gewalt oder durch Ereignisse, die durch den Auftraggeber oder den Nutzer zu verantworten sind (z.B. Warten auf Zusatzinformationen durch den Nutzer, Unterbrechung auf Nutzerwunsch, etc.).

Folgende Prioritäten werden für die Störungsbearbeitung im Rahmen der beauftragten Leistungen definiert:

Priorität	Auswirkung	Dringlichkeit	Bearbeitung
Niedrig (bisher 4)	Incident betrifft einzelne Benutzer. Die Geschäftstätigkeit ist nicht eingeschränkt.	Ersatz steht zur Verfügung und kann genutzt werden, oder das betroffene System muss aktuell nicht genutzt werden. Tätigkeiten, deren Durchführung durch den Incident behindert wird, können später erfolgen.	Priorität Niedrig führt zur Bearbeitung durch den Auftragnehmer und unterliegt der Überwachung des Lösungsfortschritts. Die Reaktionszeit (Beginn der Bearbeitung oder qualifizierter Rückruf) ergibt sich aus der Serviceklasse.
Mittel (bisher 3)	Wenige Anwender sind von dem Incident betroffen. Geschäftskritische Systeme sind nicht betroffen. Die Geschäftstätigkeit kann mit leichten Einschränkungen aufrechterhalten werden.	Ersatz steht nicht für alle betroffenen Nutzer zur Verfügung. Die Tätigkeit, bei der der Incident auftrat, kann später oder auf anderem Wege evtl. mit mehr Aufwand durchgeführt werden.	Priorität Mittel führt zur standardmäßigen Bearbeitung durch den Auftragnehmer und unterliegt der Überwachung des Lösungsfortschritts. Die Reaktionszeit (Beginn der Bearbeitung oder qualifizierter Rückruf) ergibt sich aus der Serviceklasse.
Hoch (bisher 2)	Viele Anwender sind betroffen. Geschäftskritische Systeme sind betroffen. Die Geschäftstätigkeit kann eingeschränkt aufrechterhalten werden.	Ersatz steht kurzfristig nicht zur Verfügung. Die Tätigkeit, bei der der Incident auftrat, muss kurzfristig durchgeführt werden.	Priorität Hoch führt zur bevorzugten Bearbeitung durch den Auftragnehmer und unterliegt besonderer Überwachung des Lösungsfortschritts. Die Reaktionszeit (Beginn der Bearbeitung oder qualifizierter Rückruf) ergibt sich aus der Serviceklasse.

² Gilt nicht für gesetzliche Feiertage, sowie 24.12. und 31.12.

<p>Kritisch (bisher 1)</p>	<p>Viele Anwender sind betroffen. Geschäftskritische Systeme sind betroffen. Die Geschäftstätigkeit kann nicht aufrechterhalten werden.</p>	<p>Ersatz steht nicht zur Verfügung. Die Tätigkeit, bei der der Incident auftrat, kann nicht verschoben oder anders durchgeführt werden.</p>	<p>Priorität Kritisch führt zur umgehenden Bearbeitung durch den Auftragnehmer und unterliegt intensiver Überwachung des Lösungsfortschritts. Die Reaktionszeit (Beginn der Bearbeitung oder qualifizierter Rückruf ergibt sich aus der Serviceklasse.</p>
--------------------------------	---	--	--

5 Erläuterungen

5.1 Erläuterung VDBI

V = Verantwortlich	"V" bezeichnet denjenigen, der für den Gesamtprozess verantwortlich ist. „V“ ist dafür verantwortlich, dass „D“ die Umsetzung des Prozessschritts auch tatsächlich erfolgreich durchführt.
D = Durchführung	"D" bezeichnet denjenigen, der für die technische Durchführung verantwortlich ist.
B = Beratung	"B" bedeutet, dass die Partei zu konsultieren ist und z. B. Vorgaben für Umsetzungsparameter setzen oder Vorbehalte formulieren kann. „B“ bezeichnet somit ein Mitwirkungsrecht bzw. eine Mitwirkungspflicht.
I = Information	"I" bedeutet, dass die Partei über die Durchführung und/oder die Ergebnisse des Prozessschritts zu informieren ist. „I“ ist rein passiv.

Anlage 9a zum Vertrag V5378/2300000

Security Service Level Agreement (Teil A)

Betrieb des Verfahrens Wissensmanagement für Berufliche Schulen in Hamburg (WiBeS)

für die

Behörde für Schule und Berufsausbildung (BSB)

Hamburger Straße 31

22083 Hamburg

Version 1.1
Stand: 01.09.2010

Inhaltsverzeichnis

1	Einleitung	3
1.1	Aufbau des Dokumentes	3
1.2	Leistungsgegenstand	3
2	Rahmenbedingungen	4
2.1	Rahmenbedingungen und zugrundeliegende Sicherheitsstandards	4
3	Leistungsbeschreibung	5
3.1	IT-Strukturanalyse	5
3.2	Modellierung	6
3.3	Basis-Sicherheits-Check	6
3.4	Weitere enthaltene Leistungen	7
4	Leistungsnachweis	8
4.1	Zusammenfassung: Aufbau und Inhalte des Sicherheitsnachweises	8
4.2	Abgrenzung der Leistungen	8
5	Erläuterungen und Glossar	9

1 Einleitung

Der Auftragnehmer stellt dem Auftraggeber IT Ressourcen einschließlich Hardware und systemnaher Software sowie IT Dienstleistungen mit dem vereinbarten Leistungsumfang bedarfsgerecht zur Verfügung (im Folgenden als Verfahren bezeichnet). Mit dieser Leistungsvereinbarung (Security Service Level Agreement, SSLA) wird geregelt, wie unter Informationssicherheitsgesichtspunkten der Betrieb erfolgt und wie die von Dataport im eigenen Zuständigkeitsbereich getroffenen Sicherheitsmaßnahmen dem Kunden nachgewiesen werden (Sicherheitsnachweis).

1.1 Aufbau des Dokumentes

Diese Anlage enthält die folgenden Kapitel:

Rahmenbedingungen (Kapitel 2): Regelung von Rechten und Pflichten von Auftraggeber und Auftragnehmer, Änderung bzw. Kündigung der Vereinbarung sowie Übergangsbestimmungen.

Leistungsbeschreibungen (Kapitel 3): Inhaltliche Beschreibung der vom Auftragnehmer bereitgestellten Leistungen.

Leistungsnachweis (Kapitel 4): Beschreibung des Nachweises über die erbrachten Leistungen zur Informationssicherheit.

1.2 Leistungsgegenstand

Gegenstand dieses Security Service Level Agreements sind die Nutzung des Dataport Informationssicherheitsmanagementsystems (ISMS) und die Dokumentation des Umsetzungsstandes der Sicherheitsmaßnahmen im Kundenverfahren auf Basis von IT-Grundschutz.

2 Rahmenbedingungen

2.1 Rahmenbedingungen und zugrundeliegende Sicherheitsstandards

Dataport betreibt ein Informationssicherheitsmanagementsystem (ISMS) auf Basis von IT-Grundschutz, herausgegeben durch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Der Aufbau des ISMS erfolgt auf Grundlage des BSI-Standards 100-1¹. Wesentliche Elemente des ISMS sind:

1. die Aufbauorganisation mit den im Geschäftsverteilungsplan (GVP) dokumentierten Funktionsträgern im Informationssicherheitsmanagement;
2. die im IT-Sicherheits- und Datenschutzmanagementhandbuch beschriebenen Prozesse des Informationssicherheitsmanagements, insb.
 - a. die Umsetzung der Grundschutz-Vorgehensweise auf Grundlage des BSI-Standards 100-2,
 - b. das Sicherheitsvorfallmanagement und
 - c. das Notfallmanagement sowie
3. das Dataport-Regelwerk zur Informationssicherheit.

Das ISMS stellt sicher, dass nach dem im BSI-Standard 100-2 festgelegten Schema die einschlägigen Sicherheitsmaßnahmen der IT-Grundschutz-Kataloge ausgewählt und umgesetzt werden. Es liefert dem Auftraggeber

1. die Berücksichtigung einschlägiger Grundschutzmaßnahmen bei Planung, Errichtung und Betrieb von Verfahren des Auftraggebers sowie
2. den Nachweis über aktuell umgesetzte Sicherheitsmaßnahmen (Sicherheitsnachweis).

Bei der Planung und Umsetzung von Sicherheitsmaßnahmen geht der Auftragnehmer von einem normalen Schutzbedarf für das Kundenverfahren aus. Bei abweichendem Schutzbedarf sind geeignete, über das Schutzniveau normal hinausgehende Maßnahmen im Rahmen einer Risikoanalyse durch den Auftraggeber festzulegen und beim Auftragnehmer gesondert zu beauftragen (SSLA Anlage Teil B).

¹ Eine Übersicht über die aktuelle Version der BSI-Standards findet sich unter https://www.bsi.bund.de/cfn_165/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

3 Leistungsbeschreibung

Als persönlichen Ansprechpartner für die Fortentwicklung der Sicherheitskonzeption im Kundenverfahren und als Schnittstelle in die o.g. Sicherheitsprozesse des Auftragnehmers wird ein IT-Sicherheitskoordinator (ITSK) benannt. Für das Verfahren WiBeS (Wissensmanagement für Berufliche Schulen in Hamburg) wird durch den Auftragnehmer benannt:

Funktionsträger	Mailadresse	Telefonnummer
ITSK		
Vertreter		

Die weiteren Leistungen, die der Auftragnehmer erbringt, folgen der im BSI-Standard 100-2 beschriebenen Vorgehensweise. Hierbei werden wesentliche Teile des Sicherheitskonzeptes eines Kundenverfahrens in der IT-Grundschutzsystematik erstellt (Sicherheitskonzeption) und die Umsetzung der in der Konzeption festgelegten Maßnahmen nachgewiesen (Sicherheitsnachweis). Folgende Leistungen werden im Einzelnen erbracht:

3.1 IT-Strukturanalyse

Dem Auftraggeber wird eine Übersicht über die zu seinem Verfahren gehörige IT-Infrastruktur in standardisierter Form zur Verfügung gestellt. Dies beinhaltet

1. einen verdichteten Netzplan in der IT-Grundschutzsystematik und
2. Listen der beteiligten Systeme und Netzwerkkomponenten (sog. Komponentenliste, gem. Formvorgabe im BSI-Standard 100-2).

Zur IT-Infrastruktur (auch IT-Verbund) zugehörig betrachtet werden die folgenden Infrastrukturen des Auftragnehmers:

- Dokumentation zu Aufbau und Leistungen des Informationssicherheitsmanagementsystems (ISMS);
- betroffene Gebäude und Räume beim Auftragnehmer;
- Systeme, die dem Verfahrensbetrieb dienen einschl. Managementsysteme für den Systembetrieb, die Netzinfrastruktur und administrative Clients;
- beteiligte Netzinfrastruktur beim Auftragnehmer bis zum Übergaberouter in das jeweilige Landesnetz sowie
- Anwendungen und Dienste, sofern sie in den IT-Grundschutz-Katalogen² betrachtet und vom Auftragnehmer bereitgestellt werden.

Objekte wie z.B. Gebäude, Systeme und Netzwerkkomponenten werden in allen Teilen der Dokumentation mit einem eindeutigen Kürzel bezeichnet. Dieses Kürzel findet sich sowohl im Netzplan und der Komponentenliste als auch in den nachfolgend erläuterten Reports aus der Verwaltungssoftware.

² Die aktuelle Version der IT-Grundschutz-Kataloge findet sich unter https://www.bsi.bund.de/cln_165/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

3.2 Modellierung

In Form eines Reports aus der Verwaltungssoftware (derzeit das GSTool, bereitgestellt vom BSI) weist der Auftragnehmer nach, welche Bausteine der IT-Grundschutz-Kataloge auf den IT-Verbund des Auftragnehmers und einzelne Objekte aus dem IT-Verbund angewendet werden. Die Bausteine beinhalten eine vom BSI vorgegebene Auswahl betrachteter Gefährdungslagen (Risiken) und festgelegter Sicherheitsmaßnahmen. Die Zuweisung der Bausteine erfolgt nach den in den IT-Grundschutz-Katalogen beschriebenen Regeln.

3.3 Basis-Sicherheits-Check

In Form eines weiteren Reports aus der Verwaltungssoftware weist der Auftragnehmer den Umsetzungsstand der festgelegten Sicherheitsmaßnahmen nach. Dabei folgt die Dokumentation dem vom BSI vorgegebenen Schema der Dokumentation in fünf Stufen (Ja, Teilweise, Nein, Entbehrlich, Unbearbeitet).

Dataport verpflichtet sich in den SSLA, im eigenen Zuständigkeitsbereich des Kundenverfahrens die vom BSI in den IT-Grundschutzkatalogen vorgegebenen Maßnahmen für den Schutzbedarf normal umzusetzen (Maßnahmen der Kategorien A, B und C).

Im laufenden Betrieb können bei einzelnen Maßnahmen Abweichungen auftreten, die im Basis-Sicherheits-Check berichtet werden. Ursachen für Abweichungen können sein:

- Änderungen in der IT-Infrastruktur führen im laufenden Projekt vorübergehend zu einer Abweichung von IT-Grundschutz.
- Neue IT-Grundschutzmaßnahmen, die sich aus einer Aktualisierung der IT-Grundschutzkataloge ergeben, sind noch nicht umgesetzt.
- Zur IT-Infrastruktur des Verfahrens gehören bereits vorhandene Infrastrukturen vom Auftragnehmer, die noch nicht IT-grundschutzkonform errichtet wurden bzw. betrieben werden.

Die Umsetzungsdokumentation beinhaltet:

- Hinweise auf das zugrundeliegende Regelwerk des Auftragnehmers;
- eine Beschreibung der Abweichungen von IT-Grundschutz, sofern vorhanden sowie
- den geplanten Umgang mit durch den Auftragnehmer festgestellten Abweichungen (geplantes Vorgehen und Zeitplan).

3.4 Weitere enthaltene Leistungen

Der Auftragnehmer stellt dem Auftraggeber in Ergänzung zu den genannten Dokumenten das im Umfeld des IT-Verbundes einschlägige Regelwerk auf der Ebene der Leitlinien und Richtlinien zur Verfügung. Die im Kap. 3 beschriebene Dokumentation wird in elektronischer Form zur Verfügung gestellt (üblicherweise auf CD). Auf Nachfrage des Auftraggebers wird eine aktualisierte Dokumentation zur Verfügung gestellt.

Betriebliche Detaildokumentation über die Ebene der Richtlinien hinaus wie detaillierte Netzpläne, IP-Adresskonzepte, Firewall-Policies oder Konfigurationsdateien von Systemen hält der Auftragnehmer auf Nachfrage für den Auftraggeber zur Einsicht vor Ort bereit.

Der Auftragnehmer ermöglicht dem Auftraggeber die Prüfung von Angemessenheit und Wirksamkeit der Umsetzung der IT-Grundschutz-Vorgehensweise.

Dies beinhaltet

- die Beantwortung von Fragen zur übergebenen Dokumentation über den ITSK sowie
- die Überprüfung der Umsetzung der vereinbarten Maßnahmen vor Ort beim Auftragnehmer in Begleitung durch den ITSK.

4 Leistungsnachweis.

4.1 Zusammenfassung: Aufbau und Inhalte des Sicherheitsnachweises

Der Sicherheitsnachweis des Auftragnehmers beinhaltet wesentliche Teile eines IT-grundschutzkonformen Sicherheitskonzeptes. Dies sind:

- eine kurze Einführung im Umgang mit der übergebenen Dokumentation sowie vier Verzeichnisse mit dem folgenden Inhalten:
- A0 IT-Sicherheitsrichtlinien; dies beinhaltet das im Umfeld der Vertragsgegenstandes relevante IT-Sicherheitsregelwerk zusammen mit einer Übersicht (Excel-Tabelle)
- A1 IT-Strukturanalyse; diese beinhaltet in den Anlagen neben einer Beschreibung des Gegenstandes des Sicherheitskonzeptes:
 - Komponentenlisten (Übersicht über Server und Netzwerkkomponenten)
 - Übersicht über am Verfahren beteiligte Dataport-Administratoren und deren Clients
 - Übersicht über beteiligte Netze
 - Verdichtete Netzpläne
- A3 Modellierung des IT-Verbundes (Bausteinauswahl)
- A4 Ergebnis des Basis-Sicherheitschecks

4.2 Abgrenzung der Leistungen

Die genannten, vom Auftragnehmer bereitgestellten Leistungen stellen kein vollständiges, IT-grundschutzkonformes Sicherheitskonzept dar. Fehlende Teile können insbesondere sein:

- Dokumentation spezifischer Sicherheitsanforderungen des Auftraggebers wie etwa an das Datensicherungskonzept oder das Notfallvorsorgekonzept gem. BSI-Grundschutz;
- eine Schutzbedarfsfeststellung;
- bei hohem oder sehr hohem Schutzbedarf eine ergänzende Sicherheits- und Risikoanalyse sowie die Umsetzung der daraus folgenden, über IT-Grundschutz hinausgehenden Sicherheitsmaßnahmen;
- die Sicherheitskonzeption für Teile des IT-Verbundes, die nicht unmittelbar vom Auftragnehmer betrieben werden.

Der Auftragnehmer bietet Beratung und Unterstützung für die Erstellung der hier genannten fehlenden Teile des Sicherheitskonzeptes an. Diese ist gesondert zu beauftragen.

Ebenfalls gesondert zu beauftragen sind Überprüfungen der Maßnahmenumsetzung und Audits, die über den bereitgestellten ITSK hinaus Personal beim Auftragnehmer binden. Dies sind insbesondere Audits in Anlehnung an das Prüfschema des BSI für ISO 27001 Zertifizierungen und Zertifizierungsaudits.

5 Erläuterungen und Glossar

Basis-Sicherheits-Check	Überprüfung und Dokumentation des Umsetzungsstandes der in der Modellierung festgelegten IT-Grundschutzmaßnahmen
BSI	Bundesamt für Sicherheit in der Informationstechnik
IT-Grundschutz-Kataloge	Vom BSI bereitgestellte, in Bausteine gegliederte Kataloge mit Gefährdungen (Risiken) und zugehörigen Standard-Sicherheitsmaßnahmen; die beschriebenen Sicherheitsmaßnahmen entsprechen den Anforderungen der ISO/IEC 27002
ISMS	Informationssicherheitsmanagementsystem; die Anforderungen an derartige Systeme sind den Standards ISO/IEC 27001 und BSI 100-1 beschrieben.
ITSK	IT-Sicherheitskoordinator; Ansprechpartner für Kundenanfragen und Informationssicherheitsmanagementprozesse bei Dataport
IT-Strukturanalyse	Beschreibung der zu einem (Teil-) Verfahren gehörenden IT-Infrastruktur bestehend aus einem verdichteten Netzplan und einer Übersichtsliste über beteiligte Systeme und Netzwerkkomponenten
IT-Verbund	In der IT-Strukturanalyse zu beschreibende IT-Infrastruktur zur Umsetzung eines Verwaltungsverfahrens
Modellierung	Auswahl einschlägiger Bausteine (d.h. Gefährdungen und zugehörigen Grundschutzmaßnahmen) für die Objekte in einem IT-Verbund
Sicherheitskonzept	Auch IT-Sicherheitskonzept; das formale Vorgehen nach BSI-Standard 100-2 wird eingehalten
Sicherheitskonzeption	Teil-Sicherheitskonzept, dem nach der IT-Grundschutzvorgehensweise im BSI-Standard 100-2 vorgegebene Teile fehlen können. Die Sicherheitskonzeption enthält bei Dataport in jedem Falle Maßnahmen, die nach den Modellierungsregeln des BSI ausgewählt werden.
Sicherheitsnachweis	Elektronische Dokumentation der von Dataport für das Kundenverfahren erstellten, grundschutzkonformen Sicherheitskonzeption und Dokumentation der Maßnahmenumsetzung
SSLA	Security Service Level Agreements

Security Service Level Agreement (Teil B)

Betrieb des Verfahrens Wissensmanagement für Berufliche Schulen in Hamburg (WiBeS)

für

Behörde für Schule und Berufsausbildung (BSB)

Hamburger Straße 37

22083 Hamburg

Version 1.0

Stand: 22.03.2011

Inhaltsverzeichnis

1	Einleitung	3
1.1	Überblick.....	3
1.2	Aufbau des Dokumentes.....	3
2	Zusätzliche Maßnahmen	4
2.1	Rahmenbedingungen.....	4
2.2	Festlegung geeigneter Maßnahmen.....	4
2.3	M8.1 Redundanzkonzept.....	4
2.4	M8.2 Rollen und Rechtekonzept.....	4
2.5	M8.3 Kryptokonzept.....	4
2.6	M8.4 Schnittstellenkonzept.....	4
2.7	M8.5 Mandantenkonzept.....	4
2.8	M8.6 RAS-Konzept.....	4
2.9	M8.7 Schutzschranke.....	4
2.10	M8.8 Softwarepflege.....	5
2.11	M8.9 Protokollierungskonzept.....	5
2.12	M8.10 Organisatorische Maßnahmen.....	5
3	Teilnahme an Kontrollen und Auditierungen	6
3.1	Rahmenbedingungen.....	6
3.2	Leistungsbeschreibung.....	6
4	Erläuterungen und Glossar	7

1 Einleitung

1.1 Überblick

Diese Anlage Teil B zu den SSLAs enthält ergänzende Regelungen zu Leistungen, die über die in den SSLAs vereinbarten Leistungen hinausgehen.

1.2 Aufbau des Dokumentes

Diese Anlage enthält die folgenden Kapitel:

Zusätzliche Maßnahmen (Kapitel 2):

Regelung von geeigneten, über das Schutzniveau normal hinaus gehenden Maßnahmen, die im Rahmen einer Risikoanalyse durch den Auftraggeber festgelegt wurden.

Teilnahme an Kontrollen und Auditierungen (Kapitel 3):

Inhaltliche Beschreibung der vom Auftragnehmer bei Kontrollen und Auditierungen bereitgestellten Leistungen.

2 Zusätzliche Maßnahmen

2.1 Rahmenbedingungen

Voraussetzung für die Festlegung zusätzlicher Maßnahmen ist eine vom Auftraggeber durchgeführte Risikoanalyse, auf Basis von IT-Grundschutz, herausgegeben durch das Bundesamt für Sicherheit in der Informationstechnik (BSI), in der die Maßnahmen für die Abdeckung der Gefährdungen bei hohen Schutzbedarfen ermittelt wurden.

2.2 Festlegung geeigneter Maßnahmen

Folgende Maßnahmen werden zur Abdeckung der Gefährdungslagen vereinbart:

2.3 M8.1 Redundanzkonzept

Erstellung und Umsetzung eines Redundanzkonzeptes.

2.4 M8.2 Rollen und Rechtekonzept

Fachspezifisches Rollen und Rechtekonzept sowie Berechtigungskonzept in den nutzenden Behörden unter Berücksichtigung für verschiedene Daten verarbeitende Stellen Dies beinhaltet sowohl die Belange von Nutzern als auch fachlichen Leitstelle und Dienstleister.

2.5 M8.3 Kryptokonzept

Erstellung und Umsetzung eines Kryptokonzeptes, das die Vertraulichkeit und Integrität der zu übermittelnden und zu speichernden Daten sicherstellt. Für die Infrastruktur von Dataport gilt das Dataport-Kryptokonzept.

2.6 M8.4 Schnittstellenkonzept

Erstellung eines Schnittstellenkonzeptes, das die Absicherung des Datentransfers und den Zugriff auf Daten außerhalb der Anwendung beschreibt.

2.7 M8.5 Mandantenkonzept

Erstellung und Umsetzung eines Mandantenkonzeptes für die Daten verarbeitenden Stellen.

2.8 M8.6 RAS-Konzept

Starke Authentisierung, Melde- und Sperrprozess für RAS/VPN-Einwahl; Für Administrationsarbeitsplätze (Dataport) wird für den RAS eine starke Authentisierung vorgeschrieben. Für den in diesem Umfeld eingesetzten Token gibt es einen Melde- und Sperrprozess. Die Details regelt das Dataport-RAS-Konzept.

2.9 M8.7 Schutzschränke

Einsatz von Schutzschränken im Rechenzentrum; Um den Zugriff auf die Server weiter einzuschränken, werden im Dataport-Rechenzentrum Schutzschränke eingesetzt.

2.10 M8.8 Softwarepflege

Behandlung des Themas Fehlerkorrektur in der Anwendung /Softwarepflegevertrag unter Berücksichtigung von Aspekten der Hardwarekompatibilität.

2.11 M8.9 Protokollierungskonzept

Erstellung und Umsetzung eines Protokollierungskonzeptes.

2.12 M8.10 Organisatorische Maßnahmen

Erstellung einer Konzeption und Umsetzung organisatorischer Maßnahmen außerhalb der Anwendung, die das Risiko der Aufdeckung der Identität schutzbedürftiger Personen geeignet reduzieren.

3 Teilnahme an Kontrollen und Auditierungen

3.1 Rahmenbedingungen

In den SSLAs ist geregelt, dass im Rahmen datenschutzrechtlicher Überprüfungen des Auftraggebers folgende Leistungen enthalten sind:

- die Beantwortung (bzw. das Herbeiführen der Beantwortung durch die fachlich Verantwortlichen) von Fragen zur übergebenen Dokumentation über den ITSK sowie
- die Überprüfung der Umsetzung der vereinbarten Maßnahmen vor Ort beim Auftragnehmer in Begleitung durch den ITSK.

Im Falle dass der ITSK die gestellten Fragen nicht sofort beantworten kann, erfolgt die Beantwortung zu einem späteren Zeitpunkt ggfs. auch schriftlich.

In vielen Fällen sind aber die Überprüfungen der Maßnahmenumsetzung in einem zeitlich straffen Zeitrahmen geplant. Dies hat zur Folge, dass über den bereitgestellten ITSK hinaus Personal beim Auftragnehmer gebunden werden kann. Beispiele hierfür können sein:

- Vorabkontrollen durch die Datenschutzaufsichtsbehörden
- Datenschutzauditierungen
- Audits in Anlehnung an das Prüfschema des BSI für ISO 27001
- sonstige Zertifizierungen und Zertifizierungsaudits.

Für die Durchführung solcher Kontrollen sind Terminabsprachen, sowie eine Bereitstellung der Prüft Themen mit jeweils 4 Wochen Vorlauf notwendig, um die jeweiligen Fachleute identifizieren und einplanen zu können.

3.2 Leistungsbeschreibung

In allen unter 2.1 Absatz 2 aufgeführten Kontrollen ist ein erhöhter Personalbedarf aufgrund der jeweiligen Überprüfungsschemen vorhanden.

Dataport begleitet die Kontrollen in diesen Fällen in der Regel durch:

- den IT-Sicherheitsbeauftragten
- die/den IT-Sicherheitskoordinator/in
- die IT-Sicherheitsmanager der beteiligten Bereiche
- die jeweiligen Fachleute

Diese Personen stellen – soweit nicht bereits im Rahmen der SSLA geschehen - gem. dem jeweiligen Prüfplan die Unterlagen zu den Prüft Themen zusammen, bereiten sich gezielt auf die Fragestellungen vor, und nehmen an der Prüfung teil. Dadurch werden qualitativ hochwertige Kontrollen mit zeitnahen Prüfergebnissen gewährleistet.

Die Abrechnung des über den Einsatz des ITSK hinausgehenden Personals erfolgt auf Grundlage eines Leistungsnachweises.

4 Erläuterungen und Glossar

Basis-Sicherheits-Check	Überprüfung und Dokumentation des Umsetzungsstandes der in der Modellierung festgelegten IT-Grundschutzmaßnahmen
BSI	Bundesamt für Sicherheit in der Informationstechnik
IT-Grundschutz-Kataloge	Vom BSI bereitgestellte, in Bausteine gegliederte Kataloge mit Gefährdungen (Risiken) und zugehörigen Standard-Sicherheitsmaßnahmen; die beschriebenen Sicherheitsmaßnahmen entsprechen den Anforderungen der ISO/IEC 27002
ISMS	Informationssicherheitsmanagementsystem; die Anforderungen an derartige Systeme sind den Standards ISO/IEC 27001 und BSI 100-1 beschrieben.
ITSK	IT-Sicherheitskoordinator; Ansprechpartner für Kundenanfragen und Informationssicherheitsmanagementprozesse bei Dataport
IT-Strukturanalyse	Beschreibung der zu einem (Teil-) Verfahren gehörenden IT-Infrastruktur bestehend aus einem verdichteten Netzplan und einer Übersichtsliste über beteiligte Systeme und Netzwerkkomponenten
IT-Verbund	In der IT-Strukturanalyse zu beschreibende IT-Infrastruktur zur Umsetzung eines Verwaltungsverfahrens
Modellierung	Auswahl einschlägiger Bausteine (d.h. Gefährdungen und zugehörigen Grundschutzmaßnahmen) für die Objekte in einem IT-Verbund
Sicherheitskonzept	Auch IT-Sicherheitskonzept; das formale Vorgehen nach BSI-Standard 100-2 wird eingehalten
Sicherheitskonzeption	Teil-Sicherheitskonzept, dem nach der IT-Grundschutz-vorgehensweise im BSI-Standard 100-2 vorgegebene Teile fehlen können. Die Sicherheitskonzeption enthält bei Dataport in jedem Falle Maßnahmen, die nach den Modellierungsregeln des BSI ausgewählt werden.
Sicherheitsnachweis	Elektronische Dokumentation der von Dataport für das Kundenverfahren erstellten, grundschutzkonformen Sicherheitskonzeption und Dokumentation der Maßnahmenumsetzung
SSLA	Security Service Level Agreements

