



Lastenheft

“Sanierung Stadtbad und die damit verbundene Einführung neuer Hard- und Software”

Stand: 05.07.2024

Version: 1.0

HINWEIS:

Das vorliegende Dokument enthält eine Vielzahl sehr unterschiedlicher Inhalte und Anforderungen, welche stets unter Berücksichtigung der individuellen Ziele und Rahmenbedingungen des jeweiligen Vorhabens zu bewerten, auf Anwendbarkeit und Nutzen zu prüfen und entsprechend abzuspeichern sind.

Die Erstellung eines IS-Lastenheftes sollte stets unter Federführung des ISB und niemals allein durch den entsprechenden Bedarfsträger erfolgen. Mithin handelt es sich beim vorliegenden Dokument nicht um eine klassische Dokumentvorlage.

Der ISB ist so frühzeitig wie möglich in die Erstellung eines Lastenheftes einzubeziehen und für die Erstellung des IS-Lastenheftes federführend verantwortlich.

Inhaltsverzeichnis

1	Einleitung	2
2	Ziele	2
2.1	Ziele im Sinne der Informationssicherheit	2
2.2	Geltungsbereich	2
2.3	IS-relevante Liefergegenstände Fehler! Textmarke nicht definiert.	
3	Abkürzungsverzeichnis	4
4	Anlagen	4

Dokumentvorlage „Lastenheft zur Informationssicherheit“**Anlage 11 zur Unternehmensweisung „Informationssicherheit“****1 Einleitung**

Das nachfolgende Lastenheft beschreibt informationssicherheitsspezifische Anforderungen an die Erneuerung der gesamten Hard- und Software, auf die aktuelle Sanierungsmaßnahme 2025 bis 2028 im Stadtbad der Bäder Halle GmbH.

Funktionale oder operative Anforderungen sind nicht Gegenstand dieses Lastenheftes. Das vorliegende Dokument enthält Lasten, welche der Sicherstellung eines hinreichenden Schutzniveaus im Rahmen von Planung, Implementierung und Betrieb dieser Plattform dienen.

2 Ziele

Um den Adressaten dieses Lastenheftes ein bestmögliches Verständnis für die Ziele des potentiellen Auftraggebers zu geben, werden an dieser Stelle wesentliche Ziele des geplanten Lastenheftgegenstandes erläutert.

2.1 Operative Ziel

Operative Ziele der geplanten bäderspezifischen Hard- und Softwareerneuerung sind Gegenstand des Leistungsverzeichnisses.

2.2 Ziele im Sinne der Informationssicherheit

Grundsätzliches Ziel der nachfolgenden Anforderungen ist die Gewährleistung von Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität aller Informationen, Anwendungen, IT-Systeme, Netze und Kommunikationsverbindungen im Verantwortungsbereich des Auftraggebers.

Bzgl. der geplanten bäderspezifischen Hard- und Softwareerneuerung bedeutet dies vor allem:

- den hinreichenden Schutz aller systemrelevanten Komponenten vor Manipulation und unbefugtem Zugriff
- den hinreichenden Schutz aller im geplanten System und darüber hinaus verarbeiteten schutzbedürftigen/personenbezogenen Informationen
- die Sicherstellung eines hochverfügbaren Betriebes der erforderlichen Infrastruktur

Hierzu sind hinreichende technische, organisatorische, personelle und infrastrukturelle Schutzmaßnahmen zu implementieren und ein kontinuierliches Informationssicherheitsmanagement für den nachfolgenden Betrieb aufzubauen. Die o.a. Schutzmaßnahmen müssen den Anforderungen der DIN ISO/IEC 27001 umfassend genügen.

2.3 Geltungsbereich

Die nachfolgend beschriebenen Anforderungen gelten im Verantwortungsbereich von AUFTRAGGEBER (AG) und AUFTRAGNEHMER (AN) wie folgt:

- [organisatorisch] - alle Organisationseinheiten/ Mitarbeiter des AUFTRAGNEHMERS, welche im Rahmen von Entwicklung, Einführung und Betrieb des geplanten Systems Zugriff auf schutzbedürftige Informationen, Anwendungen und IT-Systeme des Unternehmens haben
- [technisch] - die gesamte IT-Infrastruktur des geplanten Systems sowie sämtliche Informations-, Kommunikations- und Übertragungstechnik, welche im Rahmen von Entwicklung, Einführung und Betrieb des geplanten Systems schutzbedürftige Informationen der Stadtwerke Halle GmbH verarbeiten
- [infrastrukturell] - alle Einrichtungen, Objekte und Räumlichkeiten, in welchen die o.a. technischen Komponenten zum Einsatz kommen

Dokumentvorlage „Lastenheft zur Informationssicherheit“**Anlage 11 zur Unternehmensweisung „Informationssicherheit“**

- [zeitlich] - für den gesamten Zeitraum der Geschäftsbeziehung zwischen AN und AG (Einführungsprojekt, Regelbetrieb etc.) | Über die Geschäftsbeziehung hinausgehende Anforderungen werden explizit benannt.

2.3.1 Service-Level-Agreement (SLA)

Im Rahmen des vorliegenden Projektes ist ein Service-Vertrag / Service Level Agreement für den späteren Regelbetrieb abzustimmen. Im Rahmen des vorliegenden Lastenheftes zugesagte-IS Anforderungen sind auch im Regelbetrieb zu gewährleisten.

Folgende sicherheitsrelevante Themenbereiche sind zwingend abzudecken/ zu dokumentieren:

- umfassende Beschreibung IS-relevanter Leistungen, Aufgaben und Prozesse inkl. Zuweisung klarer Verantwortlichkeiten und Ansprechpartner
- Definition messbarer Leistungsmerkmale und -kennzahlen
- Organisatorische Schutzmaßnahmen
 - Organisation der Informationssicherheit
 - Zertifizierungen
 - IS-Dokumentation
 - Einhaltung geltender Sicherheitsrichtlinien des Auftraggebers
 - Compliance mit gesetzlichen Anforderungen
 - Meldepflichten
 - Kontrollrechte / Audits
 - Schwachstellenmanagement
 - Mängelabstellung
 - Kompatibilität
 - Lifecycle-Management
 - Schutz geistigen Eigentums
 - Risikomanagement
 - Über- / Rückgabe von Unternehmenswerten
 - Fernwartung / -zugriffe
 - Änderungsmanagement
 - Sichere Softwareentwicklung
 - Security-Incident und Notfallmanagement
 - Auslagerungs-/Outsourcing-Prozesse
 - Human-Resources-Security
 - Support/Supportorganisation
- Infrastrukturelle Schutzmaßnahmen
 - Zutrittskontrollmechanismen / -konzepte
 - Maßnahmen zur Ausfallsicherheit
- Technische Schutzmaßnahmen
 - Schadsoftwareschutz
 - Berechtigungsmanagement
 - Updatemanagement
 - Einsatz kryptographischer Werkzeuge
 - Datenhaltung
 - Datensicherung
 - zugelassene Hard- und Software
 - Passwort-Policy
 - Zugangskontrolle / Zugriffskontrolle
 - Authentisierungsmechanismen

Dokumentvorlage „Lastenheft zur Informationssicherheit“**Anlage 11 zur Unternehmensweisung „Informationssicherheit“**

- Protokollierung / Alarmierung
- Systemhärtung / Konfigurationsmanagement
- Schnittstellenmanagement
- Personelle Schutzmaßnahmen
 - zentraler Ansprechpartner zum Thema Informationssicherheit
 - qualifizierte Ansprechpartner
 - Verpflichtung von Mitarbeitern
 - regelmäßige Belehrung / Sensibilisierung
 - Ausscheiden eines Mitarbeiters
- Ausnahmeregelungen

3 Abkürzungsverzeichnis

AG	Auftraggeber
AN	Auftragnehmer
BSI	Bundesamt für Sicherheit in der Informationstechnik
IuK	Informations- und Kommunikationstechnik
ISm	infrastrukturelle Schutzmaßnahme
IS	Informationssicherheit
ISMS	Informationssicherheitsmanagementsystem
IuK	Informations- und Kommunikationssysteme
NEA	Netzersatzanlage
OSm	organisatorische Schutzmaßnahme
PSm	personelle Schutzmaßnahme
SFm	Schutzmaßnahmen bei Fremdhosting
SLA	Service Level Agreement
TSm	technische Schutzmaßnahme
UAN	Unterauftragnehmer
USV	Unterbrechungsfreie Stromversorgung

4 Anlagen

Anlage 1: Sicherheitstechnische Anforderungen/ Schutzmaßnahmen

Dokumentvorlage „Lastenheft zur Informationssicherheit“

Anlage 11 zur Unternehmensweisung „Informationssicherheit“

Anlage 1: Sicherheitstechnische Anforderungen/ Schutzmaßnahmen

Die nachfolgende Tabelle dokumentiert detaillierte Anforderungen an den AN bzw. normative Schutzmaßnahmen bzgl. des geplanten Liefergegenstandes. Diese basieren auf den ISO-Normen ISO/ IEC 27001:2015 (deutsch) und ISO/ IEC 27002:2017 (deutsch). Im Sinne einer besseren Übersichtlichkeit wurden allen Anforderungen eine eindeutige ID zugeordnet. Die Anforderungen sind thematisch in folgende Bereiche gruppiert:

Organisatorische Schutzmaßnahmen (OSm)

Organisatorische Schutzmaßnahmen dienen im Wesentlichen der Gewährleistung sicherer Einführungs- und Betriebsprozesse inkl. einer klaren Definition sicherheitsrelevanter Aufgaben, Anforderungen und Verantwortlichkeiten.

Infrastrukturelle Schutzmaßnahmen (ISm)

Die Gewährleistung eines hinreichenden Schutzes aller im Rahmen des o.a. Geltungsbereiches relevanten Objekte, Einrichtungen, Gebäude und Räumlichkeiten ist Ziel der in dieser Anlage beschriebenen infrastrukturellen Schutzmaßnahmen.

Technische Schutzmaßnahmen (TSM)

Technische Schutzmaßnahmen dienen im Kern der Gewährleistung einer hinreichenden technischen Härtung (sichere Hard- und Softwarekonfiguration) aller im o.a. Geltungsbereich relevanten Anwendungen, IuK-Systeme, Netze und Kommunikationsverbindungen.

Personelle Schutzmaßnahmen (PSm)

Die Belehrung, Sensibilisierung und Ertüchtigung aller gem. o.a. Geltungsbereich relevanten Personen im Sinne der Betriebs- und Informationssicherheit ist Gegenstand der nachfolgend beschriebenen personellen Schutzmaßnahmen.

Dokumentvorlage „Lastenheft zur Informationssicherheit“

Anlage 11 zur Unternehmensweisung „Informationssicherheit“

Tabelle 1: Lastenübersicht „Erneuerung Hard- und Software bzgl. Gebäudeleittechnik und Badewassertechnik“

Die nachfolgende Tabelle dokumentiert potentielle Anforderungen eines Bedarfsträgers an einen Lastenheftgegenstand/ ein geplantes System. Die Auswahl im konkreten Fall zutreffender Anforderungen sollte stets gemeinsam im IS-Gremium (ISB, IS-K, Verfahrens-/ Prozess-, Betriebs- und Assetverantwortliche) erfolgen.

Ifd. Nr.	Anforderung	Priorität a) „Muss“ b) „Kann“	Bemerkungen
1.) Organisatorische Schutzmaßnahmen			
OSm 001	Betrieb und Kontrolle eines ISMS Betreibt und überwacht der Auftragnehmer ein Managementsystem zur Informationssicherheit (ISMS), das sich an ISO-Standards der 2700x-Reihe orientiert?	Muss	Einschränkungen etc.
OSm 002	IS-Dokumentation Auf Seiten des Auftragnehmers existiert eine schriftliche / gelenkte / regelmäßig revidierte IS-Dokumentation, welche in hinreichend detaillierten Anweisungen und Richtlinien klare Anforderungen und Schutzmaßnahmen bzgl. IS- (und für den o.a. Geltungsbereich) relevanter Prozesse und Assets definiert?	Muss	Einschränkungen etc.
OSm 003	Support Der Auftragnehmer bietet eine Supportorganisation in Deutschland und in deutscher Sprache.	Muss	Einschränkungen etc.
OSm 004	Der Auftragnehmer bietet telefonischen Support mindestens wie folgt: Mo - Fr 08:00 – 17:00 Uhr.	Muss	Einschränkungen etc.
OSm 005	Der Auftragnehmer bietet die Möglichkeit zur schriftlichen Kontaktaufnahme über ein Web-Portal (z.B. via Kontaktformular) oder eine zentrale E-Mail-Adresse.	Muss	Einschränkungen etc.
OSm 006	<u>Einhaltung geltender Sicherheitsrichtlinien der SWH GmbH:</u>	Muss	Einschränkungen etc.

Dokumentvorlage „Lastenheft zur Informationssicherheit“
Anlage 11 zur Unternehmensweisung „Informationssicherheit“

Ifd. Nr.	Anforderung	Priorität a) „Muss“ b) „Kann“	Bemerkungen
	Die durch den AG an den AN in Form von IS-Belhrungen und Regelwerken übergebenen IS-Regularien und Anforderungen sind durch den AN uneingeschränkt umzusetzen. Relevante Richtlinien sind: ○ Vertraulichkeitsvereinbarung ○ "IT-Nutzerbelehrung SWH-Gruppe" (Fremdpersonal) ○ "Administratorbelehrung SWH-Gruppe" (Fremdpersonal)		
OSm 007	<u>Compliance:</u> Die Einhaltung gesetzlicher Anforderungen im Sinne der Informationssicherheit sind durch den AG uneingeschränkt sicherzustellen. Wesentliche Rechtsgrundlagen sind: ○ Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) ○ Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) ○ Datenschutzgrundverordnung (DSGVO) ○ Bundesdatenschutzgesetz (BDSG) ○ Urhebergesetz (UrhG)	Muss	Einschränkungen etc.
OSm 008	<u>Meldepflichten:</u> Erkennt der AN im Rahmen von Entwicklung, Einführung und Betrieb des geplanten Systems IS-relevante Defizite (IS-Vorfälle, Schwachstellen, unzureichende Schutzmaßnahmen, Non-Konformitäten etc.), so sind diese unverzüglich an den zentralen Ansprechpartner und den Datenschutz- / Informationssicherheitsbeauftragten des AG zu melden.	Muss	Einschränkungen etc.

Dokumentvorlage „Lastenheft zur Informationssicherheit“

Anlage 11 zur Unternehmensweisung „Informationssicherheit“

Ifd. Nr.	Anforderung	Priorität a) „Muss“ b) „Kann“	Bemerkungen
OSm 009	<u>Schwachstellenmanagement/ Mängelabstellung:</u> Erkannte Defizite, Schwachstellen, Nichtkonformitäten bzw. Risiken im Sinne der Informationssicherheit sind in Abstimmung mit dem AG schnellstmöglich und nach „best-efford“-Ansatz abzustellen. Der Abschluss derartiger Korrekturmaßnahmen ist dem AG unmittelbar zu melden.	Muss	Einschränkungen etc.
OSm 010	<u>Kontrollrechte:</u> Der AG ist jederzeit berechtigt, die Einhaltung abgestimmter Anforderungen und Schutzmaßnahmen auf Seiten des AN zu überprüfen. Entsprechende Informationen (z.B. Zertifikate) und (falls erforderlich) Zutritts-, Zugangs- und Zugriffsrechte sind dem verantwortlichen Auditor des AG bei Bedarf zur Verfügung zu stellen.	Muss	Einschränkungen etc.
OSm 011	<u>Auftragskontrolle:</u> Der Zugriff auf schutzbedürftige Informationen des AG ist ausschließlich den Mitarbeitern des AN vorbehalten, welche dies unmittelbar für die Erfüllung ihrer mit dem AG abgestimmten Aufgaben benötigen.	Muss	Einschränkungen etc.
OSm 012	<u>Schutz geistigen Eigentums:</u> Durch den AG übergebene Unterlagen, Arbeitsmittel, elektronische Daten etc. unterliegen dem Urheberrecht und sind Eigentum des AG. Sie sind nur im Rahmen der vorliegenden Beauftragung zu nutzen und nach Zweckerfüllung gem. Maßgabe des AG zurückzugeben bzw. zu vernichten.	Muss	Einschränkungen etc.
OSm 013	<u>Lizenzmanagement:</u> Zur Vermeidung von Lizenzverstößen ist durch den AG eine Gegenüberstellung der im geplanten System installierten Softwareprodukte (welches Produkt auf welchem IT-System) und der entsprechenden Lizenzurkunden zu erstellen. Lizenzurkunden sind in geeigneter Form an den AG zu übergeben.	Muss	Einschränkungen etc.

Dokumentvorlage „Lastenheft zur Informationssicherheit“

Anlage 11 zur Unternehmensweisung „Informationssicherheit“

Ifd. Nr.	Anforderung	Priorität a) „Muss“ b) „Kann“	Bemerkungen
OSm 014	Der erworbene Release der Software bzw. relevanter Softwareprodukte kann ohne zusätzliche (laufende) Kosten dauerhaft genutzt werden.	Muss	Einschränkungen etc.
OSm 015	Zwingend erforderliche und optionale laufende Kosten sind im Rahmen der Angebotsvorlage darzustellen. Beispiele hierfür sind: ○ Softwarewartungsverträge ○ Supportverträge ○ laufende Lizenzkosten etc.	Muss	Einschränkungen etc.
OSm 016	Die Lizenzbedingungen der Software bzw. relevanter Softwareprodukte und eine anforderungsgerechte Lizenzierung der Software ist Bestandteil des Angebotes.	Muss	Einschränkungen etc.
OSm 017	<u>Asset-Management:</u> Wesentlicher Liefergegenstand dieses Lastenheftes ist eine umfassende Dokumentation aller lastenheftrelevanten Assets. Gem. Maßgabe des AG ist durch den AN ein umfassendes Inventar aller im o.a. Geltungsbereich relevanten Anwendungen, IuK-Systeme (inkl. Peripherie) und sonstiger eingesetzter Technik zu erstellen. Für alle Assets sind hinreichende Betriebsunterlagen (Handbücher, Anleitungen etc.) zur Verfügung zu stellen.	Muss	Einschränkungen etc.
OSm 018	<u>sicherer Umgang mit mobilen Datenträgern:</u> Für den Fall, dass innerhalb des vorliegenden Geltungsbereiches der Einsatz mobiler Datenträger an IuK-Systemen des AG notwendig ist und der Transport schutzbedürftiger Informationen des AG auf mobilen Datenträgern jedweder Art nicht ausgeschlossen werden kann, gelten die Regularien der Sicherheitsrichtlinie "sicherer Umgang mit mobilen Speichermedien". Die wichtigsten Eckpunkte hierbei sind: ○ kein unverschlüsselter Transport vertraulicher Informationen	Muss	Einschränkungen etc.

Dokumentvorlage „Lastenheft zur Informationssicherheit“
Anlage 11 zur Unternehmensweisung „Informationssicherheit“

Ifd. Nr.	Anforderung	Priorität a) „Muss“ b) „Kann“	Bemerkungen
	kein Einsatz an IuK-Systemen des AG ohne vollständigen Malware-Scan		
OSm 019	<u>Rückgabe von Unternehmenswerten:</u> Im Rahmen der Zusammenarbeit zwischen AG und AN übergebene Unternehmenswerte des AG (IT-Systeme, Unterlagen, Speichermedien etc.) sind nach Zweckerfüllung bzw. spätestens bei Beendigung des Geschäftsverhältnisses an den AG zurückzugeben.	Muss	Einschränkungen etc.
OSm 020	<u>Vernichtung schutzbedürftiger Informationen:</u> Nicht mehr benötigte schutzbedürftige Informationen sind zuverlässig zu löschen bzw. zu vernichten, sodass eine Wiederherstellung der Daten ausgeschlossen werden kann. Dies gilt auch für die Außerbetriebnahme oder Übergabe technischer Komponenten des geplanten Systems an externe Dritte. Elektronische Daten sind ausschließlich gem. Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik zu löschen. Alternativ sind nichtflüchtige elektronische Speichermedien (z.B. Festplatten, Speicherchips etc.) durch einen zertifizierten Fachbetrieb zu vernichten (Schutzklasse 3 gem. DIN 66399). Schutzbedürftige Papierdokumente sind entweder an den AG zurückzugeben oder mit einem Shredder der Schutzklasse 3 gem. DIN 66399 zu vernichten.	Muss	Einschränkungen etc.
OSm 021	<u>Fernwartung/ -zugriffe:</u> Hinsichtlich der Fernwartung (betrifft u.a. jegliche administrativen Tätigkeiten auf Assets des vorliegenden Geltungsbereiches) gelten zusätzlich folgende Regelungen: Fernwartungsverbindungen über unsichere Kommunikationsverbindungen sind stets hinreichend abzusichern	Muss	Einschränkungen etc.

Dokumentvorlage „Lastenheft zur Informationssicherheit“
Anlage 11 zur Unternehmensweisung „Informationssicherheit“

Ifd. Nr.	Anforderung	Priorität a) „Muss“ b) „Kann“	Bemerkungen
	(Verschlüsselung, Authentisierung, sichere Deaktivierbarkeit von Fernzugängen aus unsicheren Netzen etc.). ○ Fernwartungsverbindungen sind durch den AN ausnahmslos erst nach Bestätigung der Verbindungsanfrage durch den betroffenen Nutzer des AG aufzubauen. ○ Nach Abschluss der Fernwartungsarbeiten sind die Beendigung der Remoteverbindung und das entsprechende Arbeitsergebnis durch den AN an den betroffenen Nutzer des AG zu melden. ○ Fernwartungsvorgänge sind hinreichend zu protokollieren (Systemprotokolle o.ä.). ○ Fernzugänge zur IT-Infrastruktur des AG werden ausschließlich über Sicherheitsgateways des AG realisiert. Entsprechende Anforderungen (Dienste, Protokolle, Ports etc.) sind mit dem AG und dem internen IT-Dienstleister abzustimmen.		
OSm 022	<u>Änderungsmanagement:</u> Im Rahmen der Zusammenarbeit sind zwischen AG und AN umfassende Regularien für die Durchführung IS-relevanter Änderungen an System-Komponenten und -prozessen abzustimmen. Wesentliche Aspekte sind: ○ Festlegung von Standard-Changes (keine Freigabe durch den AN erforderlich) ○ Initiierung, Planung, Prüfung, Freigabe, Kommunikation und Dokumentation von Änderungen ○ Regeln zur Absicherung von Änderungen (Testprocedere, Fallbackstrategien etc.)	Muss	Einschränkungen etc.
OSm 023	<u>Sichere Entwicklung:</u>	Muss	Einschränkungen etc.

Dokumentvorlage „Lastenheft zur Informationssicherheit“

Anlage 11 zur Unternehmensweisung „Informationssicherheit“

Ifd. Nr.	Anforderung	Priorität a) „Muss“ b) „Kann“	Bemerkungen
	Im Rahmen der Softwareentwicklung sind folgende Aspekte durch den AN zu gewährleisten: ○ Nutzung einer sicheren Entwicklungsumgebung ○ Gewährleistung sicherer Softwareentwicklungsprozesse/ -methodiken ○ Vorgabe und Einhaltung von Mindestanforderungen/ Leitlinien zur sicheren Programmierung ○ umfassende und dokumentierte Überprüfung/ Test von Entwicklungen bzgl. relevanter Sicherheitsmechanismen und Schwachstellen ○ Sicherstellung einer hinreichenden Qualifikation verantwortlicher Entwickler bzgl. sicherer Anwendungsentwicklungen und Identifikation/ Vermeidung/ Behebung IS-relevanter Schwachstellen ○ Sichere Hinterlegung von Quellcode		
OSm 024	<u>Allgemeine Dokumentation:</u> Der Liefergegenstand wird mit einer umfassenden elektronischen Dokumentation in einem handelsüblichen, bearbeitbaren Dateiformat und in deutscher Sprache ausgeliefert.	Muss	Einschränkungen etc.
OSm 025	Die Dokumentation umfasst mindestens folgende Bestandteile / deckt folgende Teilaspekte ab: ○ eine umfassende Systemdokumentation ○ eine Dokumentation verfügbarer und genutzter Schnittstellen ○ eine Anleitung zur Softwarenutzung für Anwender ○ eine Anleitung zur Softwareadministration	Muss	Einschränkungen etc.
OSm 026	<u>Vertragliche Regelung informationssicherheitsspezifischer Anforderungen:</u>	Muss	Einschränkungen etc.

Dokumentvorlage „Lastenheft zur Informationssicherheit“

Anlage 11 zur Unternehmensweisung „Informationssicherheit“

Ifd. Nr.	Anforderung	Priorität a) „Muss“ b) „Kann“	Bemerkungen
	Ist der Bieter (im Falle bzw. im Nachgang einer Beauftragung) damit einverstanden, alle durch ihn zugesagten IS- spezifischen Anforderungen, Schutzmaßnahmen, Aufgaben und Verantwortlichkeiten des vorliegenden Lastenheftes ○ zu den ebenfalls vom Bieter dargelegten Kosten ○ für den gesamten Zeitraum der Beauftragung/Zusammenarbeit (hier: das avisierte Einführungsprojekt und nachgelagerte Serviceleistungen) in einem gesonderten Service Level Agreement „Informationssicherheit“ schriftlich zuzusichern?		
2.) Infrastrukturelle Schutzmaßnahmen			
ISm 001	<u>Zutrittskontrollkonzept:</u> Räume und Gebäude des AN, welche dem o.a. Geltungsbereich zuzuordnen sind, sind durch angemessene Zutrittskontrollmechanismen und physische Barrieren vor dem Zutritt Unbefugter zu schützen.	Muss	Einschränkungen etc.
ISm 002	<u>Schutz vor äußeren Einflüssen:</u> Alle technischen Komponenten des geplanten Systems sind zuverlässig vor einem Ausfall aufgrund externer Einflüsse zu schützen.	Muss	Einschränkungen etc.
3.) Technische Schutzmaßnahmen			
TSm 001	<u>Schadsoftwareschutz:</u> Alle IT-Systeme des AN im o.a. Geltungsbereich sowie alle IT-Komponenten des geplanten Systems sind mit einem adäquaten Schadsoftwareschutz auszustatten. Wesentliche Anforderungen hierbei sind: ○ Aktualität von Software und Virensignatur (mindestens tagesaktuell) ○ regelmäßiger Scan aller Datenbestände des Systems	Muss	Einschränkungen etc.

Dokumentvorlage „Lastenheft zur Informationssicherheit“
Anlage 11 zur Unternehmensweisung „Informationssicherheit“

Ifd. Nr.	Anforderung	Priorität a) „Muss“ b) „Kann“	Bemerkungen
	○ Aktivierung der Funktionalität „on access scan“ zur Gewährleistung einer Echtzeitprüfung aller verarbeiteten Dateien		
TSm 002	<u>Berechtigungsmanagement:</u> Die Zugriffs-/ Zugangskontrolle auf schutzbedürftige Daten des geplanten Systems werden über ein entsprechendes Rollen- und Rechtekonzept gesteuert. Die Rollen werden hierbei ausnahmslos personenbezogenen Nutzerkonten zugewiesen.	Muss	Einschränkungen etc.
TSm 003	<u>Sicherheitsupdates:</u> Für die o.a. Software werden (nach Erkennen einer Schwachstelle) Sicherheitsupdates zur Verfügung gestellt. Das kontinuierliche Schließen erkannter Sicherheitslücken durch den Hersteller ist sichergestellt.	Muss	Einschränkungen etc.
TSm 004	<u>Updatemanagement:</u> Die zeitnahe Bereitstellung von Updates für IT-Systeme, Betriebssysteme/ -umgebungen, Schutzsoftware und kritische Anwendungen des geplanten Systems ist essentiell für das Schließen identifizierter Sicherheitslücken. Im Rahmen von Einführung und Produktivbetrieb sind Updates durch den AN bzgl. Kompatibilität bzw. Funktionalität zu testen und nach entsprechender Abstimmung mit dem AG systemseitig einzuspielen.	Muss	Einschränkungen etc.
TSm 005	<u>Datenhaltung:</u> Die Speicherung schutzbedürftiger Daten des AG auf Komponenten des geplanten Systems oder des AN darf stets nur dort erfolgen, wo ein hinreichender Zugriffsschutz und eine bedarfsgerechte Datensicherung sichergestellt ist. Eine wirksame Trennung von Daten anderer Informationseigentümer/ Kunden ist durch den AN sicherzustellen. Eine Datenhaltung durch externe (nicht explizit vertraglich geregelte) Cloud-Dienstleister (z.B. Dropbox, Google Drive etc.) ist verboten.	Muss	Einschränkungen etc.

Dokumentvorlage „Lastenheft zur Informationssicherheit“
Anlage 11 zur Unternehmensweisung „Informationssicherheit“

Ifd. Nr.	Anforderung	Priorität a) „Muss“ b) „Kann“	Bemerkungen
Tsm 006	<u>Datensicherung:</u> Auf IT-Komponenten des geplanten Systems oder des AN gespeicherte, schutzbedürftige System-/ Nutz- und Protokollinformationen des AG sind stets anforderungsgerecht zu sichern. Hierbei sind folgende Parameter zwischen AG und AN abzustimmen und schriftlich zu dokumentieren: ○ Verfügbarkeitsanforderungen (max. akzeptabler Datenverlust, max. tolerierbare Ausfallzeit) ○ Fristen (Aufbewahrungs-/ Löscho-/ Regenerationsfristen) ○ Schutzbedarf der Daten und sonstige Anforderungen betroffener Geschäftsprozesse ○ Sicherungs- und Wiederherstellungswerkzeuge und entsprechende Verantwortlichkeiten Prozesse, Verantwortlichkeiten und abgestimmte Datensicherungsparameter sind in IS-Dokumentation des Systems und SLA für den Regelbetrieb zu berücksichtigen.	Muss	Einschränkungen etc.
Tsm 007	<u>zugelassene Hard- und Software:</u> Die Verarbeitung schutzbedürftiger Informationen des AG ist ausschließlich auf hinreichend geschützter/ gehärteter Informations- und Kommunikationstechnik gestattet. Wesentliche Anforderungen hierbei sind: ○ ein aktueller Schadsoftwareschutz (Schutzsoftware u. Malware-Signaturen) ○ ein aktueller Stand der Sicherheitsupdates aller Soft- und Firmware-Komponenten ○ ein wirksamer und aktueller Schutz gg. externe Angreifer (Firewall etc.)	Muss	Einschränkungen etc.

Dokumentvorlage „Lastenheft zur Informationssicherheit“
Anlage 11 zur Unternehmensweisung „Informationssicherheit“

Ifd. Nr.	Anforderung	Priorität a) „Muss“ b) „Kann“	Bemerkungen
	○ eine sichere/ gehärtete Grundkonfiguration ○ wirksame Authentisierungs- und Zugangskontrollmechanismen		
TSm 008	Eine automatisierte Prüfung der o.a. Kriterien ist technisch sicherzustellen. Eine Offenlegung von Passwörtern ggü. unbefugten Dritten ist unter allen Umständen zu verhindern. Besteht der Verdacht der Offenlegung durch Unbefugte, ist unverzüglich eine Änderung des Passworts zu veranlassen. Änderung und Rücksetzung von Passwörtern bedürfen stets einer sicheren Authentifizierung des Beantragenden. Müssen durch ein Fachverfahren / IT-System (z.B. im Rahmen eingesetzter Authentifizierungsverfahren) Passwörter systemseitig gespeichert oder übertragen werden, so darf dies nie im Klartext, sondern ausschließlich als Hash-Wert unter Anwendung eines sicheren und aktuellen Hash-Verfahrens erfolgen. Werden vollständige Passwörter (z. B. in einem elektronischen Passwortsafe) gespeichert, so sind sichere Verschlüsselungsalgorithmen nach Stand der Technik einzusetzen (z.B. AES mit einer Schlüsseltiefe von mind. 256 Bit). Initialpasswörter sind stets zu ändern.	Muss	Einschränkungen etc.
TSm 009	<u>Zugangskontrolle:</u> Alle schutzbedürftigen Informationen, Anwendungen und technischen Komponenten sind mit wirksamen Zugriffs-/ Zugangskontrollmechanismen auszustatten. Die Zugangs-/ Zugriffskontrollmechanismen des geplanten Systems sind darzustellen und in der IS-Dokumentation des geplanten Systems zu berücksichtigen.	Muss	Einschränkungen etc.

Dokumentvorlage „Lastenheft zur Informationssicherheit“

Anlage 11 zur Unternehmensweisung „Informationssicherheit“

Ifd. Nr.	Anforderung	Priorität a) „Muss“ b) „Kann“	Bemerkungen
TSm 010	<u>Authentisierungsmechanismen:</u> Zutritts-, Zugangs- und Zugriffskontrollmechanismen müssen über starke Authentisierungsverfahren verfügen. Wesentliche Kriterien sind: ○ sichere Identitätsverifizierung ○ keine unverschlüsselte Übertragung von Authentisierungsdaten ○ neutrale Optik (keine Offenlegung kritischer Anmeldeinformationen) ○ technische Durchsetzung der Passwort-Policy ○ begrenzte Anzahl von Anmeldeversuchen ○ Protokollierung ○ Verwendete Authentisierungsmechanismen sind darzustellen.	Muss	Einschränkungen etc.
TSm 011	<u>Systemhärtung/ Konfigurationsmanagement:</u> Alle Komponenten des geplanten Systems sind durch den AN hinreichend zu härten (Deaktivierung/ Deinstallation nicht erforderlicher Dienste, max. Einschränkung der Zugangs- und Zugriffsrechte, sichere Konfiguration der Systeme und Anwendungen, Einsatz zusätzlicher Härtungsmaßnahmen etc.).	Muss	Einschränkungen etc.
TSm 012	<u>Protokollierung/ Alarmierung:</u> Sicherheitsrelevante Ereignisse bzw. Zustände des geplanten Systems (z.B. kritische Systemparameter, Hardwareversagen, kritische Systemzustände, Anmeldevorgänge, Konfigurationsänderungen, System- und Nutzeraktivitäten etc.) sind zu protokollieren. Sicherheitskritische Ereignisse sollten in Echtzeit zu einer Alarmierung/ Meldung führen (z.B. via E-Mail oder als Warnmeldung im System). Protokolldaten sind gem. Maßgabe des AG vor unbefugtem Zugriff zu schützen. Eine zentrale Synchronisation der Systemzeiten ist sicherzustellen.	Muss	Einschränkungen etc.

Dokumentvorlage „Lastenheft zur Informationssicherheit“

Anlage 11 zur Unternehmensweisung „Informationssicherheit“

Ifd. Nr.	Anforderung	Priorität a) „Muss“ b) „Kann“	Bemerkungen
TSm 013	<u>Netzwerksicherheit:</u> Im Rahmen einer ggf. notwendigen Einrichtung / Anpassung des Netzwerkes des AG sind folgende Aspekte zwischen AN und AG abzustimmen und in Netzbetriebs-/ Netzwerksicherheits-/ Netzwerkmanagementkonzept zu dokumentieren: ○ Netz-/ Netzstrukturpläne ○ erforderliche Netzwerkdienste (nicht benötigte Dienste und Protokolle sind zu deaktivieren) ○ Zugangskontrollmechanismen und Zugangsmittel für den Zugang zu Netzwerken und Netzwerkdiensten (z. B. Nutzung von VPN)	Muss	Einschränkungen etc.
TSm 014	<u>Schutz gg. Angriffe:</u> Es ist sicherzustellen, dass die eingesetzten Softwarekomponenten Sicherheitsmaßnahmen gegen Angriffe zur Verfügung stellen (z.B. Eingabekontrollen oder Code-Injection). Details sind durch den Auftragnehmer darzulegen.	Muss	Einschränkungen etc.
TSm 015	<u>Änderungshistorie:</u> Die umfassende und (wo immer möglich) automatisierte Dokumentation von Änderungen am geplanten System ist wesentliche Voraussetzung für Nachvollziehbarkeit und Transparenz sicherheitsrelevanter Vorgänge. Das System bietet Werkzeuge zur automatisierten Dokumentation sicherheitsrelevanter Änderungsvorgänge (Changes).	Muss	Einschränkungen etc.
TSm 016	<u>Fehlermeldungen:</u> Die Software bietet Funktionalitäten, welche Non-Konformitäten bzgl. vordefinierter Prozesse, Zustände oder Daten identifizieren.	Muss	Einschränkungen etc.

Dokumentvorlage „Lastenheft zur Informationssicherheit“

Anlage 11 zur Unternehmensweisung „Informationssicherheit“

Ifd. Nr.	Anforderung	Priorität a) „Muss“ b) „Kann“	Bemerkungen
4.) Personelle Schutzmaßnahmen			
PSm 001	<u>qualifizierte Ansprechpartner:</u> Für alle im Rahmen von Entwicklung, Einführung und Betrieb des geplanten Systems relevanten Aufgaben des AN sind ausschließlich hinreichend qualifizierte Mitarbeiter einzusetzen. Stellvertreter oder Nachfolger sind eigenständig, zeit- und bedarfsgerecht zu benennen und zu ertüchtigen.	Muss	Einschränkungen etc.
PSm 002	<u>Aus- und Weiterbildung / Systemeinstrweisung:</u> Vor Inbetriebnahme des geplanten Systems sind alle relevanten Mitarbeiter von AN und AG umfassend und zielgruppengerecht in die für sie relevanten Komponenten und deren sichere und korrekte Bedienung einzuweisen. Ein entsprechender Schulungsplan ist schriftlich durch den AN zu dokumentieren.	Muss	Einschränkungen etc.
PSm 003	<u>Ausscheiden eines Mitarbeiters:</u> Verlassen Mitarbeiter des AN den o.a. Geltungsbereich oder ändert sich das Aufgabenspektrum (z.B. bei Kündigung oder interner Versetzung), sind relevante Zutritts-, Zugangs- und Zugriffsrechte bedarfsgerecht anzupassen (i.d.R. Entzug der Rechte). Unternehmenswerte bzw. Zutritts-, Zugangs- und Zugriffsmedien (Schlüssel, Zugangsdaten etc.) sind einzuziehen bzw. zu ändern.	Muss	Einschränkungen etc.