Inhaltsverzeichnis

Anlage 1 Mindestanforderungen Dienstleister mit PIT-Zugang – Selbstauskunft

A.1 Anwendung

Anwendung findet die Selbstauskunft bei Dienstleistern im PIT-Umfeld, die direkt oder über Fernzugang auf Ressourcen zugreifen oder zugreifen sollen und über kein zertifiziertes ISMS verfügen.

Für die in den folgenden Kapiteln genannten Mindestanforderungen sind – wo gefordert – die Umsetzungsstände („umgesetzt“ oder „nicht umgesetzt“) auszuwählen und die Umsetzungsniveaus (Art der Umsetzung) zu beschreiben. Die Darstellung des jeweiligen Umsetzungsniveaus kann direkt in der Selbstauskunft oder in einem formlosen Dokument erfolgen. Verfügt der Dienstleister über eigene Richtlinien, so kann bei den betreffenden Mindestanforderungen auf die entsprechenden Stellen in den Richtlinien ergänzend hingewiesen werden. Die Richtlinien sowie ggf. weitere Dokumente sind sodann der Selbstauskunft anzuhängen.

A.2 Allgemeine Anforderungen

Für einen angemessenen Umgang mit Fragen der Informationssicherheit sind grundsätzliche Regelungen im Hause des Dienstleisters erforderlich. Die gesetzlichen Bestimmungen des Datenschutzes und das Telekommunikationsgeheimnis sind einzuhalten. Alle Informationen über Daten und Vorgänge, die bei der Durchführung des Auftrages bekannt werden, sind auch nach Beendigung des Vertrages vertraulich zu behandeln.

A.3 Organisation

A.3.1 Benennung eines Ansprechpartners für Informationssicherheit

Es ist ein zentraler Ansprechpartner zu benennen, der verbindliche Auskünfte zur Informationssicherheit – sowohl im internen Bereich als auch im Außenverhältnis zum Auftraggeber – geben kann. Für den Fall der Abwesenheit ist eine Vertretung bekanntzugeben. Änderungen in der Verantwortlichkeit oder in den Kontaktdaten sind dem Auftraggeber unverzüglich mitzuteilen.

Kontaktdaten:

_____

_____

_____

A.3.2 Berücksichtigung der Informationssicherheit

Die Informationssicherheit ist im Rahmen der Beauftragung und während der Zusammenarbeit gewährleistet, beispielsweise durch die Formulierung umzusetzender Anforderungen und/oder durch die Einbeziehung des o. g. Ansprechpartners für Informationssicherheit.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.3.3 Umgang mit Informationssicherheitsvorfällen

Der Dienstleister ist verpflichtet alle Ereignisse, welche die Schutzziele (auch potentiell) des Auftraggebers gefährden, unverzüglich zu melden. Entsprechende Verfahren und vordefinierte Schnittstellen zur Meldung solcher Ereignisse existieren.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.3.4 Zugriffsschutz für IT-Komponenten

Alle IT-Komponenten, von denen unmittelbar oder mittelbar ein Zugriff auf Ressourcen im Bereich der Prozess-IT des Auftraggebers möglich ist, müssen mit einem Zugriffsschutz versehen sein. Dabei ist gleichermaßen der physische Zugriff als auch der logische Zugang zu schützen. Es sind die bereits vom Betriebssystem vorgegebenen Mechanismen zur Authentisierung zu nutzen. Die eingesetzte Authentisierungsmethode sollte die Vergabe von komplexen Kennworten mit hoher Kennwortgüte Mindestwortlänge, Groß-/Kleinschrift, Sonder- und Zahlzeichen) ermöglichen. Auslieferungskennwörter dürfen nicht auf Systeme im produktiven Einsatz übernommen werden. Authentifizierungsinformationen sind an keiner Stelle im Klartext abzulegen. Eine entsprechende Kennwortrichtlinie muss vorliegen. Das Booten von bootfähigen Datenträgern sowie die parallele Installation mehrerer Betriebssysteme sind zu verhindern.

Durch geeignete organisatorische und technische Maßnahmen ist sicherzustellen, dass nur namentlich benannte Mitarbeiter Zugang zu diesen Ressourcen des Auftraggebers erhalten.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.3.5 Verbot der privaten Nutzung

Alle IT-Komponenten, von denen unmittelbar oder mittelbar ein Zugriff auf Ressourcen des Auftraggebers möglich ist, dürfen nur für dienstliche Zwecke genutzt werden. Eine private Nutzung durch die Mitarbeiter ist nicht zulässig. Private IT-Komponenten dürfen ebenfalls nicht für den Zugriff auf Systeme des Auftraggebers benutzt werden bzw. nicht an Systeme bzw. Netze des Dienstleisters angeschlossen werden, die für den Zugriff auf Ressourcen des Auftraggebers vorgesehen sind.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.3.6 Notfallvorsorge

Der Dienstleister hat ein BCM (Business Continuity Management) etabliert, das im Rahmen einer Notfalls oder einer Krise die Aufrechterhaltung einer Mindest-Servicequalität und die schnellstmögliche Wiederherstellung aller für den Auftraggeber bereitzustellenden Dienste sicherstellt.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.4 Umgang mit Informationen

Alle Informationen und Daten, die dem Dienstleister im Rahmen seiner Tätigkeit bekannt werden bzw. anfallen, müssen vertraulich behandelt werden. Ausgenommen hiervon sind nur offensichtlich nicht vertrauliche Informationen. In Zweifelsfällen hat der Dienstleister eine Klassifizierung durch die Auftraggeber anzufordern. Die Informationen müssen entsprechend ihrer Klassifikation behandelt werden. Dies gilt insbesondere bei der Übertragung über öffentliche Netze, beim Versand via Briefpost oder E-Mail und bei der Speicherung auf mobilen Datenträgern. Daten (in elektronischer und/oder gedruckter Form), die nicht mehr benötigt werden, müssen nicht wiederherstellbar gelöscht bzw. zerstört werden.

A.4.1 Informationsverarbeitung außerhalb der EU

Für alle Informationen und Daten, die dem Dienstleister im Rahmen seiner Tätigkeit bekannt werden bzw. die er verarbeitet, ist sicherzustellen, dass sie nicht in ein Land außerhalb der EU übertragen, dort verarbeitet oder gespeichert werden.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.4.2 Speicherung

Sofern vertrauliche oder sicherheitsrelevante Daten auf externen oder mobilen Geräten (beispielsweise Notebooks oder Speichermedien) gespeichert werden, müssen die Daten kryptographisch nach dem Stand der Technik verschlüsselt werden. Sofern die Daten auf externen Datenträgern gespeichert werden, hat der Dienstleister für den physikalischen Schutz und die sichere Verwahrung Sorge zu tragen. Zur Sicherung der Arbeitsergebnisse sind geeignete Sicherungen anzufertigen, die genauso zu sichern sind.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.4.3 Datenübertragung

Sofern vertrauliche oder sicherheitsrelevante Daten über öffentliche oder anderweitig nicht vertrauenswürdige Netze übertragen werden, muss die Übertragung kryptographisch nach dem Stand der Technik, gemäß der Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI), verschlüsselt werden.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.4.4 E-Mail-Versand

Vertrauliche oder sicherheitsrelevante Daten dürfen per E-Mail nur versendet werden, wenn sie kryptographisch nach dem Stand der Technik, gemäß der Empfehlungen des BSI, verschlüsselt wurden.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.4.5 Reparatur und Entsorgung von IT-Komponenten und Systemen

Werden Systeme und IT-Komponenten, die vertrauliche Daten enthalten, zur Reparatur oder Entsorgung gegeben, so ist die durchgängige Wahrung der Vertraulichkeit der Informationen durch sichere Löschung oder Zerstörung der Speichermedien zu gewährleisten.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.5 Mitarbeiter und ggf. eingesetzte Unterauftraggeber

Etwaige Unterauftragsverhältnisse müssen vom Dienstleister offengelegt und vom Auftraggeber freigegeben werden.

Zusätzlich sind neben den Einweisungen durch den Auftraggeber die Mitarbeiter des Dienstleisters und evtl. Unterauftragnehmer bzgl. grundsätzlicher Regelungen zur Informationssicherheit zu schulen und auch zu verpflichten.

A.5.1 Vertraulichkeitsvereinbarung

Die Mitarbeiter (eigene und Mitarbeiter evtl. Unterauftragsverhältnisse) sind durch ihren Arbeitsvertrag bzw. getrennte Verpflichtungserklärungen auf Vertraulichkeit und Einhaltung der datenschutzrechtlichen Bestimmungen auch über das Ende ihrer Beauftragung hinaus zu verpflichten.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.5.2 Sicherheitsunterweisung

Die Mitarbeiter sind über die sicherheitstechnischen Anforderungen der IT-Ressourcen des Auftraggebers zu informieren. Das betrifft insbesondere die möglichen Risiken, adäquate Gegenmaßnahmen sowie die persönlichen Verantwortungen der Mitarbeiter im Rahmen ihrer Tätigkeiten. Zusätzlich sind die Mitarbeiter in Bezug auf Informationssicherheit regelmäßig durch entsprechende Schulungen oder Mitteilungen zu unterweisen. Hierzu gehören auch sicherheitsbezogene Informationen bei Einführung neuer Techniken und Verfahren.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.5.3 Abmeldung

Die Mitarbeiter sind zu verpflichten, sich nach Aufgabenerfüllung vom IT-System bzw. von der IT-Anwendung abzumelden.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.5.4 Ausscheiden von Mitarbeitern

Beim Ausscheiden von Mitarbeitern des Dienstleisters ist durch geeignete Maßnahmen sicherzustellen, dass der weitere Zugang zu Systeme und Anwendungen des Auftraggebers durch ausgeschiedene Mitarbeiter verhindert wird.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.6 Netzwerksicherheit

Die Gewährleistung der Informationssicherheit im Netzwerk des Dienstleisters ist auch für den Auftraggeber wichtig, da im Rahmen der Dienstleister-Erbringung in der Regel Informationen und Applikationen entweder direkt durch Netzkopplung oder indirekt durch Service-PCs oder Datenträger in die Einrichtungen des Auftraggebers gelangen bzw. übertragen werden.

A.6.1 Schutz des internen Netzes durch eine Firewall

Das interne IT-Netzwerk des Dienstleisters ist gegenüber externen IT-Netzen am Netzübergang mindestens durch eine Firewall nach dem Stand der Technik zu schützen. Ein einfacher Paketfilter gilt nicht als ausreichend. Die Firewall darf nur explizit benötigte und freigegebene Dienste erlauben.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.6.2 Extern erreichbare Dienste und Remote-Access ins interne Netz

Direkte Zugriffe aus dem Internet in das interne Netz sind nicht zulässig und müssen von der Firewall unterbunden werden. Sofern Remote-Access (RAS) in das interne Netz des Dienstleisters erforderlich ist oder Dienste vom Internet aus erreichbar sein müssen (z. B. Webserver, Mailserver etc.), darf eine Umsetzung erst nach einer dokumentierten Sicherheitsanalyse erfolgen. Die Ergebnisse dieser Analyse sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.6.3 Kabellose Netze

Der Einsatz von kabellosen Netzen darf nur bei angemessener Sicherung, insbesondere durch starke Authentisierung und Verschlüsselung, gemäß Stand der Technik und den Empfehlungen des BSI, erfolgen.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.7 Malwareschutz / Sicherheitsupdates

Der Dienstleister hat ein wirksames Virenschutzkonzept und Patch-Management für seine IT-Komponenten im eigenen Hause zu etablieren, das dem jeweils aktuellen Stand der Technik entspricht und kontinuierlich der technischen Entwicklung angepasst wird.

A.7.1 Virenschutz am Arbeitsplatz

Der Einsatz eines Virenscanners auf allen Arbeitsplatzrechnern ist verpflichtend. Die Überprüfung muss dabei automatisch beim Zugriff auf Dateien (auch verschlüsselte) erfolgen und darf vom Benutzer nicht unterbunden werden können. Zusätzlich sind alle Arbeitsplatzrechner regelmäßig auf eventuell vorhandene Viren zu prüfen.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.7.2 Zusätzlicher Virenschutz

Neben dem Virenschutz am Arbeitsplatz sind Viren-Scanner im Gateway- bzw. Serverbereich zur Überprüfung der bei E-Mail, Filetransfer (z. B. FTP) und Webverkehr übertragenen Daten als auch bei mobilen Wartungsgeräten einzusetzen.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.7.3 Regelmäßige Aktualisierung der Virenpattern

Der Virenschutz ist aktuell zu halten. Die Virenschutzprogramme müssen über die Möglichkeit des automatisierten Downloads von Viren-Pattern verfügen. Das Update der Virenpattern muss mindestens einmal pro Tag durchgeführt werden.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.7.4 Einspielen von Sicherheitsupdates

Sicherheitsupdates für das Betriebssystem und für Kommunikationsprogramme, mit denen auf Internetdienste zugegriffen wird, müssen auf allen Systemen umgehend eingespielt werden. Ebenso sind die Firewall und alle öffentlich erreichbaren Server auf aktuellem Stand zu halten. Sicherheitsupdates sind auf diesen Systemen ebenfalls umgehend einzuspielen.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.8 Wartungssysteme und Fernzugang

Der Ausdruck „Wartung“ bezieht sich in diesem Dokument allgemein auf alle vom Auftraggeber beauftragten Servicemaßnahmen, wie Instandhaltungsarbeiten, Störungsanalysen, Fehler- und Störungsbehebung, Verbesserungen, Anpassungen usw. Die Wartungssysteme, mittels derer der Dienstleister Zugang auf die PIT-Systeme des Auftraggebers sowie auf Netze und Komponenten, die direkt oder indirekt an das Prozessnetz gekoppelt werden (z. B. für Wartungszwecke), erhält, müssen besonders hohen Sicherheitsstandards genügen. Dies gilt auch für mobile Geräte, wie z. B. Laptops, Tablets, Programmiergeräte und Speichermedien wie USB-Sticks. Neben den oben geforderten allgemeinen Anforderungen sind deshalb zusätzlich die im Folgenden aufgeführten Maßnahmen umzusetzen.

A.8.1 Allgemeine Anforderungen Fernzugang

Der Fernzugang zur Prozessumgebung des Auftraggebers, z. B. zu Fernwartungszwecken, darf generell nur über die vom Auftraggeber zur Verfügung gestellten und genehmigten Zugangsmöglichkeiten erfolgen. Auf Seiten des Dienstleisters darf der Fernzugang nur durch einen definierten, geschulten Personenkreis mit personalisierten Accounts und von speziell gesicherten Systemen aus erfolgen. Der interaktive Fernzugang wird durch die Auftraggeber im Servicefall manuell freigegeben. Nach Beendigung der Tätigkeit muss eine Abmeldung beim Auftraggeber erfolgen. Für automatisierte Abläufe des Dienstleisters, die über den Fernzugang ausgeführt werden, sind spezielle Kennungen einzurichten, die nur die vorgesehenen Funktionen ausführen können und die keinen interaktiven Zugang ermöglichen.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.8.2 Physikalische Sicherheit

Die für den Zugriff benötigten IT-Komponenten sind durch entsprechende Maßnahmen vor unberechtigten physischen Zugriff zu schützen, beispielsweise durch Installation in verschlossenen Räumen mit angemessenem Zugangsschutz oder Lagerung in verschlossenen Schränken bei Nichtbenutzung.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.8.3 Grundsicherung und Systemhärtung

Alle Systeme und Netzwerk-Komponenten müssen anhand anerkannter Best-Practice-Konzepte nach aktuellem Stand der Technik gehärtet und mit aktuellen Service-Packs und Sicherheitspatches versehen sein. Unnötige Benutzer, Programme, Netzwerkprotokolle, Dienste und Services sind zu deinstallieren, oder – falls eine Deinstallation nicht möglich ist – dauerhaft zu deaktivieren und gegen versehentliches Reaktivieren zu schützen. Die sichere Grundkonfiguration der Systeme muss überprüft und dokumentiert sein.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.8.4 Zugangsschutz

Durch geeignete organisatorische und technische Maßnahmen ist sicherzustellen, dass nur speziell autorisierte Mitarbeiter auf den Fernzugang zugreifen können. Die Zugänge zu entsprechenden Systemen müssen so restriktiv wie möglich gehandhabt und dokumentiert werden. Falls ein Mitarbeiter seinen Aufgabenbereich wechselt oder das Unternehmen des Dienstleisters verlässt, muss sichergestellt sein, dass die entsprechenden Zugangsberechtigungen unmittelbar entzogen wird.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.8.5 Sichere Administrations- und Wartungstools

Die eingesetzten Tools unterstützen eine personalisierte Anmeldung, kryptographischen Schutz der Passwörter, optional eine starke Authentisierung und eine Rechteverwaltung mit Einschränkung des Zugriffs auf den erforderlichen Umfang.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.8.6 Wartungssysteme mit direktem Fernzugriff

Erfolgt der Zugriff von Wartungssystemen nicht aus der gesicherten Umgebung des Dienstleisters heraus, sondern direkt über Internet- bzw. Einwahlverbindungen, so ist dies dem Auftraggeber vorher anzuzeigen. In einem solchen Fall muss zusätzlich zu den o. g. Maßnahmen das System zwingend über eine Firewallsoftware verfügen, die unberechtigte Zugriffe von außen verhindert. Die Firewall darf vom Benutzer nicht deaktivierbar sein. Zusätzlich erlaubt der Dienstleister dem Auftraggeber vor der Produktivsetzung als auch anlassbezogen einen koordinierten Penetrationstest durchzuführen.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____

A.8.7 Wartungssystemen zur Vor-Ort-Wartung

Auf Wartungssystemen, insb. auf mobilen Geräten, die vor Ort direkt an Prozessnetze oder -komponenten angeschlossenen werden, muss eine Firewallsoftware installiert sein, die unberechtigte Zugriffe von außen verhindert. Die Firewall darf vom Benutzer nicht deaktivierbar sein. Alternativ muss sichergestellt werden, dass diese Wartungssystemen nie direkt an unsichere Netze wie z. B. das Internet angeschlossen werden.

- ☐ umgesetzt
- ☐ nicht umgesetzt

_____

_____

_____