Erklärung zur Informationssicherheit

1. Zweck

Dieses Dokument enthält Informationssicherheitsanforderungen an Lieferanten und Dienstleister (Auftragnehmer), die Produkte und Leistungen für den OOWV (Auftraggeber) zur Verfügung stellen und in diesem Zusammenhang Zugriff auf Informationen erhalten oder Technologien bereitstellen und/oder betreiben. Durch Berücksichtigung dieser Informationssicherheits-anforderungen sollen die Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität für Informationen und Technologien des OOWV über die gesamte Dauer der Vertragsbeziehung und 2 Jahre darüber hinaus sichergestellt werden.

2. Geltungsbereich

Die in diesem Dokument festgelegten Anforderungen gelten verbindlich für alle Beschäftigten des Auftragnehmers (sowie ggf. auch für Beschäftigte von Unterauftragnehmern, siehe Ziffer 3.3), welche

- Zugriff auf bzw. Zugang zu Informationen und/oder Technologien des OOWV erhalten und/oder
- Informationen des OOWV verarbeiten und/oder
- Technologien für den OOWV bereitstellen und/oder betreiben und/oder
- Zutritt zu Räumlichkeiten des OOWV erhalten.

Sofern bereits Vereinbarungen in Bezug auf Informationssicherheitsanforderungen bestehen, die den Vorgaben aus diesem Dokument entgegenstehen, ist die Ansprechperson beim OOWV zu informieren, um schnellstmöglich eine Klärung herbeizuführen. Im Zweifel gilt die restriktivere Vorgabe.

Alle Beschäftigten des Auftragnehmers sind mit dem Inhalt dieser Vereinbarung in geeigneter Weise vertraut zu machen, bevor sie Zugriff auf Informationen oder Technologien im Geltungsbereich dieses Dokuments erhalten. Dies gilt entsprechend für künftige Beschäftigte des Auftragnehmers.

Verträge mit weiteren Lieferanten und Dienstleistern oder sonstigen Dritten (z. B. „Sub-Dienstleister“, „Nachunternehmer“, „Unterauftragnehmer“) unterliegen ebenfalls ohne Ausnahme dieser Vereinbarung.

Sofern nicht anders angegeben, sind mit „Informationen und Technologien“ immer solche Informationen und Technologien gemeint, die in Bezug zum OOWV stehen bzw. beim OOWV zum Einsatz kommen, so dass ein unzureichender Schutz dieser Informationen und Technologien zu Beeinträchtigungen der Informationssicherheit beim OOWV führen kann.

Der Begriff „Technologie“ umfasst jede Komponente, die in der Lage ist, Informationen zu verarbeiten. Also neben der klassischen Informations- und Kommunikationstechnologie (IT, IuK) und den betrieblichen Einrichtungen zur Steuerung und Überwachung unserer kritischen Dienstleistungen (OT, ICS) ggf. auch Leuchtmittel und Kaffeemaschinen, sofern diese in der

Lage sind, Informationen zu speichern und/oder mit anderen „intelligenten“ Komponenten zu teilen.

Diese Verpflichtung gilt über die gesamte Dauer der (vorvertraglichen) Vertragsbeziehung und 2 Jahre darüber hinaus.

3. Anforderungen an die Zusammenarbeit

3.1. Kommunikations- und Meldewege

Auftraggeber und Auftragnehmer benennen verantwortliche Ansprechpersonen sowie mindestens ein*e Vertreter*in, welche die Erfüllung der Lieferung bzw. Dienstleistung koordinieren.

Jegliche Kommunikation hat über die vereinbarten Ansprechpersonen zu erfolgen.

Sofern es beim Auftragnehmer zu Informationssicherheitsvorfällen kommt, ist unverzüglich die Ansprechperson bzw. die verantwortliche Stelle beim OOWV zu informieren. Das gilt entsprechend für relevante Schwachstellen gemäß Ziffer 4.4. Näheres ist unter Ziffer 3.4 geregelt.

3.2. Mitteilung des Schutzbedarfs und Ableitung von Maßnahmen

Der OOWV teilt dem Auftragnehmer schriftlich mit, welcher Schutzbedarf hinsichtlich

- Vertraulichkeit,
- Integrität und
- Verfügbarkeit

für die betroffenen Informationen und Technologien durch den OOWV festgelegt wurde.

Der Auftragnehmer ist verpflichtet, den mitgeteilten Schutzbedarf zu berücksichtigen und geeignete Maßnahmen abzuleiten.

Der Auftragnehmer teilt dem OOWV mit, durch welche Maßnahmen der durch den OOWV festgelegte Schutzbedarf von Informationen und Technologien gewährleistet wird. Diese Maßnahmen werden zwischen dem OOWV und dem Auftragnehmer abgestimmt und dokumentiert.

Änderungen des Schutzbedarfes werden dem Auftragnehmer durch die Ansprechperson des OOWV mitgeteilt, um bei Bedarf die Maßnahmen im Rahmen des Änderungsmanagements dem Schutzbedarf anzupassen.

OOWV und Auftragnehmer stimmen sich auf Grundlage der Klassifizierungsvorgaben des OOWV über den Umgang mit Informationen/Dokumenten ab. Weichen die Klassifizierungskriterien von OOWV und Auftragnehmer voneinander ab, ist eine generische Zuordnung der Vertraulichkeitsklassen durchzuführen und den Beschäftigten des Auftragnehmers (siehe Ziffer 2) bekannt zu geben.

Sofern (auch) personenbezogene Daten verarbeitet werden sollen, ist ggf. zusätzlich ein Vertrag zur Auftragsverarbeitung nach der DSGVO zu schließen.

Liegen im Einzelfall vom OOWV keine Informationssicherheitsanforderungen bzw. keine Einschätzung zum Schutzbedarf der betroffenen Informationen und Technologien vor, so hat der Auftragnehmer den Schutzbedarf selbst nach dem Stand der Technik sowie eigenen Kenntnissen und Erfahrungen festzulegen. Diese Festlegung gilt so lange, bis der OOWV eigene Anforderungen kommuniziert.

3.3. Unterauftragnehmer

Der Auftragnehmer nimmt bei der Erfüllung seiner vertraglichen Verpflichtungen gegenüber dem Auftraggeber keinen (Unter-)Unterauftragnehmer ohne vorherige schriftliche Zustimmung des OOWV in Anspruch.

Alle (Unter-)Unterauftragnehmer, die vom Auftragnehmer oder von einem seiner Unterauftragnehmer beauftragt wurden, sind auf die Einhaltung der in diesem Dokument festgelegten Sicherheitsanforderungen sowie ggf. darüber hinaus gesondert vereinbarter spezifischer Anforderungen (siehe Ziffer 5) vertraglich zu verpflichten.

Der Auftragnehmer ist gegenüber dem OOWV für die Überwachung seiner Unterauftragnehmer verantwortlich sowie für die Einhaltung der von ihm an die Unterauftragnehmer weitergereichten Anforderungen.

Art und Umfang der Arbeiten der Unterauftragnehmer sowie die Messkriterien zur Überprüfung der Leistungserbringung sind vom Auftragnehmer zu dokumentieren.

Bei einer Bietergemeinschaft hat jedes einzelne Mitglied der Bietergemeinschaft die Vorgaben dieses Dokuments einzuhalten.

3.4. Umgang mit Informationssicherheitsvorfällen

Störungen und Vorfälle beim Auftragnehmer (oder einem der (Unter-)Unterauftragnehmer) sind gemäß der folgenden Tabelle zu klassifizieren und unter Beachtung der in der Tabelle angegebenen Reaktionszeiten an die entsprechende(n) Stelle(n) beim OOWV zu melden (in der Regel ist das die Stelle, für die die beauftragte Leistung erbracht wird, sowie ggf. die zentrale Meldestelle sicherheitsvorfall@oowv.de).

Störungen und Vorfälle liegen vor, wenn die Informationssicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit entgegen dem Schutzbedarf vorübergehend oder auf Dauer nicht eingehalten werden oder nicht eingehalten werden können.

Sofern (auch) eine Verletzung des Schutzes personenbezogener Daten vorliegt, hat der Auftragnehmer unverzüglich eine Meldung an die zentrale Meldestelle des OOWV (sicherheitsvorfall@oowv.de) zu senden, unabhängig von der Störungsklasse.

Für alle übrigen Störungen und Vorfälle finden die folgenden Störungsklassen Anwendung:

Störungsklasse	Störungsdefinition für externe Dienstleister	Reaktionszeit	Meldungsweg	Meldungsannahme beim OOWV
niedrig	Störung oder Vorfall mit *möglicher* negativer Beeinflussung des Normalzustands, Ursache und deren Behebungsmöglichkeit sind *bekannt*	nächster Arbeitstag	E-Mail	<<Ansprechperson OOWV>>
hoch	Störung oder Vorfall mit *möglicher* negativer Beeinflussung des Normalzustands, Ursache und deren Behebungsmöglichkeit sind *unbekannt*	unverzüglich	E-Mail, Telefon	Zentraler Meldepunkt: sicherheitsvorfall@oowv.de UND <<Ansprechperson OOWV>>
sehr hoch	Störung oder Vorfall mit negativer Beeinflussung des Normalzustands, Ursache und deren Behebungsmöglichkeit sind *bekannt*	unverzüglich	E-Mail, Telefon	Zentraler Meldepunkt: sicherheitsvorfall@oowv.de UND <<Ansprechperson OOWV>>
kritisch	Störung oder Vorfall mit negativer Beeinflussung des Normalzustands, Ursache und deren Behebungsmöglichkeit sind *unbekannt*	unverzüglich	E-Mail, Telefon	Zentraler Meldepunkt: sicherheitsvorfall@oowv.de UND <<Ansprechperson OOWV>>

Die Meldung sollte mindestens die folgenden Informationen enthalten:

- Störungsklasse, falls bereits bekannt
- Einschätzung, welche Informationen des OOWV (möglicherweise) betroffen sind
- Einschätzung, welche Technologien des OOWV (möglicherweise) betroffen sind
- Zeit für Interimslösung (z. B. Workaround), falls bereits bekannt
- Zeit für finale Lösung (z. B. Patch), falls bereits bekannt
- Ansprechpartner*in für Rückfragen zur Meldung

3.5. Anforderungen an die Informationssicherheit des Auftragnehmers

Zugangs- und Zugriffsberechtigungen werden durch den OOWV nur in dem Umfang und für die Dauer erteilt, wie sie zur Aufgabenerfüllung erforderlich sind.

Berechtigungen für den Zugriff auf bzw. Zugang zu Informationen und Technologien sowie für den Zutritt zu Räumlichkeiten sind durch den Auftragnehmer personalisiert zu vergeben und zu dokumentieren. Abweichungen hiervon bedürfen der schriftlichen Genehmigung durch den OOWV für den jeweiligen Einzelfall.

Der Auftragnehmer hat sicherzustellen, dass die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen und Technologien gewährleistet ist.

Falls durch den Auftragnehmer ein Fernzugriff auf Technologien erforderlich ist, ist dieser – sofern nicht anders vereinbart – durch starke, den aktuellen Standards entsprechende Authentifizierungsmechanismen (2-Faktor-Authentifizierung) zu schützen.

Für diese Art des Zugriffs ist eine verschlüsselte Kommunikationsverbindung zu nutzen. Darüber hinaus gelten die durch den OOWV bereitgestellten Fernzugriffsvereinbarungen.

Sofern für die vom Auftragnehmer eingesetzten Technologien ein spezifisches Sicherheitsniveau vorgegeben ist (Ziffer 5), darf dieses vom Auftragnehmer nicht unterschritten werden. Werden durch den Auftragnehmer Technologien für den OOWV bereitgestellt, bedürfen Änderungen an der Sicherheitsarchitektur oder -konfiguration von Technologien der vorherigen Abstimmung.

Der Auftragnehmer erklärt sich damit einverstanden, dass beim (Fern-)Zugriff auf Firmendaten, welche sich auf Systemen des OOWV befinden, ein Monitoring durch den OOWV erfolgt.

3.6. Audits

Der OOWV behält sich vor, innerhalb der Dauer der Vertragsbeziehung Audits bei dem Auftragnehmer sowie ggf. bei dessen (Unter-)Unterauftragnehmern durchzuführen oder durchführen zu lassen.

Der Auftragnehmer ist verpflichtet, ihm bekannt gewordene Nicht-Konformitäten bzw. in Zertifizierungsaudits festgestellte Abweichungen zur Norm unverzüglich dem OOWV mitzuteilen, sofern sie sich auf die Informationssicherheit beim OOWV auswirken können.

3.7. Anforderungen von Dritten

Der OOWV ist als Betreiber einer Kritischen Infrastruktur beim BSI (Bundesamt für Sicherheit in der Informationstechnik) registriert. Damit unterliegen der OOWV sowie ggf. auch die von ihm in Anspruch genommenen Lieferanten und Dienstleister bestimmten gesetzlichen Vorgaben, z. B. hinsichtlich der Einhaltung des Stands der Technik und bezüglich Mitwirkungspflichten der jeweiligen Lieferanten und Dienstleister im Fall einer Beeinträchtigung der Kritischen Dienstleistung.

3.8. Ahndung von Verstößen

Bei schuldhaften Verstößen bzw. nicht genehmigten Abweichungen gegen die Vorgaben dieser Erklärung ist der OOWV zum Rücktritt vom Vertrag bzw. zur außerordentlichen Kündigung des bestehenden Vertrages berechtigt.

3.9. Beendigung des Vertragsverhältnisses

Am Ende der Vertragsbeziehung hat der Auftragnehmer alle Informationen, Dokumente und Daten des OOWV sowie zur Nutzung bereitgestellte Hard- und Software an den OOWV zu übergeben.

Nach Aufforderung durch den OOWV sind diese auf allen Datenträgern des Auftragnehmers unverzüglich zu löschen.

Die Löschung der Informationen und Daten (auch von Backups) ist durch den Auftragnehmer mit einer geeigneten Methode durchzuführen und gegenüber dem OOWV nachzuweisen.

4. Grundsätzliche Anforderungen an den Auftragnehmer

4.1. Beschaffung, Reparatur, Wartung, Außerbetriebnahme

Der Auftragnehmer verpflichtet sich, die zur Verarbeitung von Informationen des OOWV vom Auftragnehmer eingesetzten Technologien stets auf dem Stand der Technik zu halten und geeignete Maßnahmen insbesondere zum Schutz vor Malware sowie zum Schutz vor Datenverlust zu treffen.

Wird Hardware mit Daten des OOWV zur Wartung oder Reparatur an Dritte (auch Kurierdienste) weitergegeben, sind alle sensiblen Informationen, die sich auf Datenträgern befinden, vorher sicher zu löschen oder die persistenten Datenträger aus dem Gerät zu entfernen.

Wird ein Gerät außer Betrieb genommen, sind die Daten des OOWV nach vorheriger Übergabe an den OOWV sicher zu löschen bzw. die Datenträger gemäß ihrem Schutzbedarf sicher zu entsorgen.

Werden vom Auftragnehmer Technologien für den OOWV bereitgestellt, gilt zudem das Folgende:

Zur Sicherstellung einer einwandfreien Funktionalität aller Technologien, die für den OOWV bereitgestellt werden, darf durch den Auftragnehmer ausschließlich getestete und durch den OOWV freigegebene Hard- und Software sowie Firmware eingesetzt werden.

Änderungen (z. B. Wartungen, Reparaturen) an den beim OOWV eingesetzten Technologien dürfen nur zu vorher angekündigten und durch den OOWV genehmigten Zeitpunkten durchgeführt werden.

4.2. Datensicherung / Backup

Der Auftragnehmer verpflichtet sich, die Verfügbarkeit aller für die Auftragserfüllung gegenüber dem OOWV relevanten Daten und Informationen sicher zu stellen und eine Wiederherstellbarkeit in angemessener Zeit zu gewährleisten, so dass länger anhaltende Unterbrechungen des Betriebs bei Verlust oder Beschädigung von Daten und Informationen vermieden werden.

4.3. Notfallkonzepte und Maßnahmen

Für bereitgestellte Services und/oder Technologien müssen Notfallkonzepte und Notfallmaßnahmen zur Fortführung und Wiederherstellung des Betriebes erarbeitet, umgesetzt und getestet bzw. geübt werden.

Die Ansprechperson beim OOWV ist zu Beginn der Zusammenarbeit sowie bei Änderungen darüber zu informieren, wie der Auftragnehmer im Notfall zu erreichen ist.

4.4. Schwachstellenmanagement

Die Verantwortung für die Steuerung von technischen Schwachstellen, die im Einflussbereich des Auftragnehmers liegen, liegt beim Auftragnehmer.

Auftragnehmer müssen die bereitgestellten Produkte, Technologien und Services in geeigneter Weise einer kontinuierlichen Prüfung auf technische Schwachstellen unterziehen, um

- die technischen Schwachstellen zu erfassen,
- die Auswirkungen und Risiken der Schwachstellen unverzüglich zu beurteilen und
- entsprechende Abhilfemaßnahmen zu ergreifen.

Jede Schwachstelle, die sich auf die Informationssicherheit beim OOWV auswirken kann, ist vom Auftragnehmer an die Ansprechperson beim OOWV (laut Ziffer 3.4) zu melden und bezüglich möglicher funktionaler und sicherheitsrelevanter Auswirkungen zu bewerten.

Erkannte Schwachstellen und Abhilfemaßnahmen sind zu dokumentieren. Sofern es sich um Schwachstellen handelt, die sich merklich auf die Informationssicherheit beim OOWV auswirken können oder bereits zu Beeinträchtigungen in der Auftragserfüllung geführt haben, sind die Maßnahmen mit der Ansprechperson sowie dem Response-Team des OOWV abzustimmen.

Beispiele für in diesem Sinne relevante Schwachstellen sind im Anhang A aufgeführt.

4.5. Dokumentation und Berichterstattung

Alle Tätigkeiten aus den o. g. Informationssicherheitsanforderungen sind durch den Auftragnehmer zu dokumentieren. Auf Nachfrage des OOWV ist während der Dauer der Vertragsbeziehung der durch den OOWV benannten Ansprechperson sowie den Mitgliedern des Response-Teams des OOWV Einsicht in diejenigen Teile der Dokumentation zu gewähren, die im Zusammenhang mit den Informationssicherheitsanforderungen aus diesem Dokument stehen.

Beispiele für in diesem Sinne relevante Teile der Dokumentation sind im Anhang A aufgeführt.

Der OOWV ist darüber hinaus unaufgefordert über wesentliche Änderungen zu informieren, sofern sich diese direkt oder indirekt auf die Informationssicherheit beim OOWV auswirken können.

Beispiele für in diesem Sinne relevante Änderungen sind im Anhang A aufgeführt.

4.6. Sichere Kommunikationswege

Grundsätzlich sind Daten und Dokumente über die vom OOWV zur Verfügung gestellten Kommunikationswege (z. B. Share IT) auszutauschen. Wird von diesem Grundsatz abgewichen und stellt der Auftragnehmer eigene Kommunikationswege zur Verfügung, hat dieser eine angemessene Verschlüsselung nach dem Stand der Technik sicherzustellen.

4.7. Wahrung der Vertraulichkeit

Der Auftragnehmer hat sicherzustellen, dass sensible Informationen ausschließlich an Personen weitergegeben werden, die diese im Rahmen der Erfüllung der vertraglich festgelegten Leistungen benötigen (Need-to-Know-Prinzip).

Im Übrigen gelten die Regelungen der Vertraulichkeitsverpflichtungserklärung bzw. der Geheimhaltungsverpflichtungserklärung, die ebenfalls Bestandteil des zwischen Auftragnehmer und Auftraggeber geschlossenen Vertrages.

4.8. Datenschutz

Erhält der Auftragnehmer im Rahmen der Ausschreibung oder Vertragsbeziehung Zugang zu personenbezogenen Daten, die dem Auftraggeber oder Kunden des Auftraggebers zuzurechnen sind, sind vom Auftragnehmer die geltenden Datenschutzvorschriften zu beachten, insbesondere die Zweckbestimmung. Der Auftragnehmer hat sicher zu stellen, dass seine Beschäftigten sowie vom ihm beauftragte Dritte nur in dem Umfang Zugriff auf die Daten erhalten, wie es für die Auftragserfüllung zwingend erforderlich ist.

Die personenbezogenen Daten sind vom Auftragnehmer dem Stand der Technik entsprechend zu schützen und dürfen nur innerhalb des Gebietes der Bundesrepublik Deutschland, eines Mitgliedsstaates der Europäischen Union oder eines Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum (EWR) verarbeitet werden, sofern es nicht ausdrücklich anderweitig schriftlich zwischen Auftraggeber und Auftragnehmer vereinbart wurde.

Der Auftragnehmer hat seine Beschäftigten schriftlich auf das Datengeheimnis zu verpflichten und sie über die einzuhaltenden Datenschutzvorschriften zu belehren.

Dem Datenschutzbeauftragten des Auftraggebers sind auf Verlangen alle geforderten Auskünfte zu erteilen sowie ggf. Nachweise zu erbringen und geforderte Unterlagen zu übergeben.

Werden personenbezogene Daten durch den Auftragnehmer im Auftrag des Auftraggebers verarbeitet, ist ein Vertrag zur Auftragsverarbeitung abzuschließen, bevor der Auftragnehmer

Zugriff auf die personenbezogenen Daten des Auftraggebers erhält. Vorzugsweise wird der Vertrag zur Auftragsverarbeitung dem Auftragnehmer vom Auftraggeber zur Verfügung gestellt.

5. Schlussbestimmung

Der Auftragnehmer ist verpflichtet, die vereinbarten Informationssicherheitsanforderungen vollständig umzusetzen.

Abweichungen von den vereinbarten Anforderungen sind

- nur in begründeten Fällen zulässig,
- unter Einbindung des Response-Teams mit dem OOWV abzustimmen und
- schriftlich zu dokumentieren.

Dieses Dokument ist vom Auftragnehmer unterschrieben bzw. digital signiert an die Ansprechperson beim OOWV zu übergeben.

6. Bestätigung des Auftragnehmers

Mit seiner Unterschrift erklärt der Auftragnehmer die Kenntnisnahme der Vorgaben der Informationssicherheit sowie die Einhaltung dieser Vorgaben.

Ort	Datum	Auftragnehmer: *Name, Funktion / Firmenstempel / Unterschrift*

A. Anhang: Beispiele zu Ziffer 4

Beispiele zu Ziffer 4.4: Relevante Schwachstellen

- *Schwachstelle ermöglicht unberechtigten Zugriff (lesend/schreibend) auf Informationen oder Technologien*
- *Schwachstelle kann zu Datenverlust führen*
- *Schwachstelle ermöglicht Verbreitung von Malware*
- *Schwachstelle kann bewirken, dass ein Service nicht wie vereinbart zur Verfügung steht*
- *usw.*

Beispiele zu Ziffer 4.5: Relevante Teile der Dokumentation

- *Umgang mit technischen Schwachstellen*
- *Absicherung von Fernzugriffen*
- *Meldung von Sicherheitsereignissen*
- *Zugangssteuerung*

- *Verwaltung von Anmeldeinformationen*
- *Aufbewahrung von Schlüsseln*
- *Patchmanagement*
- *usw.*

Beispiele zu Ziffer 4.5: Relevante Änderungen

- *Umzug des Auftragnehmers in neue Räumlichkeiten*
- *Verlagerung von Services an andere Standorte (insbesondere in Nicht-EU-Länder)*
- *Austausch von Technologien beim Auftragnehmer*
- *Änderungen der Sicherheitsarchitektur oder -konfiguration der im Rahmen der Auftragserfüllung durch den Auftragnehmer genutzten Technologien und Services*
- *usw.*