Sicherheitsvereinbarung für Auftragnehmer

zwischen

Bundesdruckerei GmbH
Kommandantenstraße 18
10969 Berlin

- nachfolgend „Auftraggeber“ genannt – und

dem im Zuschlagsschreiben namentlich bezeichneten Unternehmen

- nachfolgend „Auftragnehmer“ genannt –

Präambel:

Diese Sicherheitsvereinbarung legt die Sicherheitsanforderungen und Maßnahmen zur Risiko-minimierung fest, die mit dem Zutritt, Zugang und Zugriff von Dienstleistern und Lieferanten – im folgenden Auftragnehmer - auf materielle und immaterielle (Informationen und Daten) Werte des Auftraggebers bzw. der Nutzung von IT-Infrastrukturen des Auftraggebers im Zusammenhang stehen.

Begriffsbestimmungen:

Ereignis der Informationssicherheit	Ein Ereignis der Informationssicherheit liegt vor, wenn der Verdacht besteht, dass die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen gefährdet ist oder beeinträchtigt werden könnte.
Vorfall der Informationssicherheit	Bei einem Vorfall der Informationssicherheit wurde bereits die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen beeinträchtigt. Weitere sicherheitsrelevante Ereignisse sind z. B. Beschädigung, Verlust oder Diebstahl von materiellen Werten oder auch Sabotage.

Sicherheitsverletzungen	Ereignisse und Vorfälle zur Sicherheit werden im Folgenden zusammenfassend als Sicherheitsverletzungen bezeichnet.
Technische und organisatorische Maßnahmen zur Sicherheit	Zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie zum Schutz vor Diebstahl, Verlust oder Beschädigung materieller Werte sind dem Leistungsgegenstand angemessene technische Maßnahmen umzusetzen. Neben technischen Maßnahmen (z. B. Verschlüsselung, Virenschutz, etc.) sind organisatorische Maßnahmen (z. B. Regelung zur Informationsweitergabe, „4-Augen-Prinzip" etc.) entsprechend der Vorgaben des Auftraggebers umzusetzen.
Mitarbeitende des Auftragnehmers	Als Mitarbeitende des Auftragnehmers werden im nachfolgenden alle Personen und Subunternehmen bezeichnet, die im Auftrag des Auftragnehmers die vereinbarte Leistung erbringen.

1. Meldepflicht von Sicherheitsverletzungen

1. Der Auftragnehmer ist verpflichtet, jede ihm bekannt gewordene Sicherheitsverletzung, die im Zusammenhang mit der Leistungserbringung steht, dem benannten Ansprechpartner des Auftraggebers zu melden. Die Meldung hat in jedem Einzelfall unverzüglich nach Kenntnisnahme zu erfolgen. Der Auftragnehmer verpflichtet seine Mitarbeitenden entsprechend.

2. Sollte der Auftragnehmer oder seine Mitarbeitenden im Rahmen der Leistungserbringung Zugriff auf Informationen des Auftraggebers erlangen, die nicht für die Bearbeitung des Auftrages notwendig sind, so ist dies unverzüglich dem Ansprechpartner des Auftraggebers anzuzeigen.

Gleiches gilt für Sicherheitsverletzungen, die in den Infrastrukturen des Auftragnehmers auftreten und folglich die Werte oder Sicherheit des Auftraggebers betreffen (z. B. Cyberangriffe auf die Kommunikationssysteme des Auftragnehmers, Abfluss von Informationen des Auftraggebers aus den Infrastrukturen des Auftragnehmers etc.).

2. Informationssicherheit in Projekten

Der Auftragnehmer ist verpflichtet, technische und organisatorische Maßnahmen zur Sicherheit inkl. Informationssicherheit und deren Dokumentation durch alle Projektphasen hindurch von Beginn an zu berücksichtigen. Die Sicherheitsanforderungen der vorliegenden Sicherheitsvereinbarung und ggf. weitere projektspezifische Anforderungen des konkreten Auftrages sind durch den Auftragnehmer nach den Vorgaben des Auftraggebers im Laufe der Leistungserbringung umzusetzen und zu beachten. Hierbei ist eine Schutzbedarfsanalyse für die im Rahmen des Auftrages bearbeiteten Informationen des Auftraggebers schon in der Planungsphase des Projektes durchzuführen und zu dokumentieren.

3. Maßnahmen VOR Leistungserbringung

3.1 Training und Awareness

Für Mitarbeitende des Auftragnehmers ist initial eine erfolgreich durchgeführte Sicherheitsunterweisung entsprechend der Vorgaben des Auftraggebers Voraussetzung für das Betreten der Liegenschaften des Auftraggebers und die Nutzung der IT-Infrastrukturen des Auftraggebers bzw. den Zugriff auf dessen Informationen. Eine Auffrischung ist nach einem mit dem Auftraggeber abgestimmten Zeitraum notwendig. Der Auftraggeber betreibt ein Lern-Management-System (LMS), das Teil des Konzeptes zur Sensibilisierung für die Sicherheit ist. Die erfolgreiche Durchführung ist für jeden einzelnen Mitarbeitenden durch ein automatisch generiertes Zertifikat nachzuweisen. Alternativ und ergänzend wird der Auftragnehmer seine Mitarbeitenden auf Anforderung des Auftraggebers anweisen, an weiteren nachweislichen Unterweisungen des Auftraggebers teilzunehmen.

Der Nachweis der durchgeführten Sicherheitsunterweisungen ist Voraussetzung für die Leistungserbringung durch den Auftragnehmer.

3.2 Social Engineering

Der Auftragnehmer ist verpflichtet, seine Mitarbeitenden darüber in Kenntnis zu setzen, welche Sicherheitsrisiken im Bereich Social Engineering vorhanden sind. Er hat in diesem Zusammenhang dafür Sorge zu tragen, dass eine entsprechende Sicherheitsverletzung vermieden wird.

Unter anderem ist auf Folgendes hinzuweisen:

1. Informationen des Auftraggebers, von denen der Auftragnehmer und seine Mitarbeitenden Kenntnis erlangen, dürfen ohne Einwilligung des Auftraggebers nicht an Dritte weitergegeben werden.
2. Passwörter oder weitere Angaben zur Authentifizierung dürfen durch den Auftragnehmer und seine Mitarbeitenden nicht weitergegeben werden. IT-Personal des Auftraggebers wird nie danach fragen!
3. Der Auftragnehmer und seine Mitarbeitenden sind aufgefordert, bei Beantwortung einer E-Mail die E-Mail-Adresse des Adressaten auf Korrektheit zu prüfen, um Fehlleitungen von Informationen des Auftraggebers zu vermeiden.
4. Wenn der Auftragnehmer oder seine Mitarbeitenden von unbekannten Personen nach Informationen des Auftraggebers oder über den Auftrag befragt werden, sind keine Informationen weiterzugeben und dies dem Ansprechpartner des Auftraggebers zu melden. Auch telefonisch sind keine Informationen des Auftraggebers an unbekannte Personen (Werbeanrufer, etc.) weiterzugeben.
5. Der Auftragnehmer und seine Mitarbeitenden sind aufgefordert, auch im privaten Umfeld keine Informationen des Auftraggebers oder den Auftrag betreffend weiterzugeben.
6. Bei internen Telefonaten im Telefonie-System des Auftraggebers ist durch den Auftragnehmer und seinen Mitarbeitenden die Kennung eines Anrufers auf dem Telefondisplay vor Informationsweitergabe zu prüfen.
7. Sind im Rahmen der Leistungserbringung Informationen des Auftraggebers intern zu versenden, sollten Dokumente nicht als Anhang in einer E-Mail, sondern stattdessen als Link mit entsprechend dahinterliegenden Berechtigungssteuerung versendet werden. Damit wird verhindert, dass irrtümlich verschickte sensible Daten durch Unberechtigte eingesehen werden können.
8. Der Auftragnehmer und seine Mitarbeitenden sind aufgefordert, sich auch im Umgang mit internen Mitarbeitenden oder anderen Auftragnehmern umsichtig zu verhalten und ggf. beobachtetes ungewöhnliches Verhalten an den Ansprechpartner des Auftraggebers zu melden.

4. Maßnahmen WÄHREND der Leistungserbringung

4.1 Verhalten auf dem Gelände des Auftraggebers

1. Der Auftragnehmer stellt sicher, dass seine Mitarbeitenden von den Inhalten dieser Sicherheitsvereinbarung sowie den für die Leistungserbringung relevanten Sicherheitsrichtlinien und Verfahrensanweisungen des Auftraggebers Kenntnis erhalten haben, diese Regelungen verstehen und einhalten (s. a. Abschnitt 3.1).
2. Der Auftragnehmer verpflichtet sich, für die Leistungserbringung im Umfeld Informationsverarbeitung nur fachlich geeignetes sowie ausreichend geschultes Personal einzusetzen.
3. Der Auftragnehmer ist darüber informiert, dass private Gegenstände, die nicht eindeutig vom Eigentum des Auftraggebers zu unterschieden sind, nur nach vorheriger Einwilligung des Ansprechpartners des Auftraggebers mitgeführt werden dürfen und bei Betreten des Geländes dem Werkschutz vorzulegen sind.
4. Zur Überprüfung der Einhaltung der Vorgaben, werden beim Verlassen des Betriebsgeländes stichprobenartige Taschenkontrollen durch den Wachdienst durchgeführt. Der Auftragnehmer und seine Mitarbeitenden unterstützen dies durch ihre Kooperation.

4.2 Informationssicherheit

4.2.1 Allgemeine Regelungen

1. Der Auftragnehmer ist informiert, dass die Einhaltung dieser Sicherheitsvereinbarung Vertragsbestandteil ist.
2. Der Auftragnehmer benennt einen Ansprechpartner für den Auftraggeber zu Fragestellungen der Informationssicherheit im Rahmen der Leistungserbringung (Informationssicherheitsbeauftragter o. ä.).
3. Dem Auftragnehmer ist bekannt, dass die Nichtbeachtung der Vorgaben zur Informationssicherheit den Entzug von Zutritt-, Zugangs- und Zugriffsrechten auf Informationen des Auftraggebers zur Folge haben kann. Daneben / Darüber hinaus stehen dem Auftraggeber bei Verletzung bei Verletzung dieser Sicherheitsvereinbarung Rechte aus dem Vertrag zu.
4. Der Auftragnehmer weist seine Mitarbeitenden an, sich im Umfeld Informationssicherheit an die Vorgaben des Auftraggebers zu halten, sofern diese im Zusammenhang mit der Leistungserbringung stehen.
5. Dem Auftragnehmer ist bekannt, dass die Infrastruktur des Auftraggebers ausschließlich für auftragsbezogene Zwecke verwendet werden darf. Der Auftragnehmer muss seine Mitarbeitenden darauf hinweisen.
6. Der Auftragnehmer verpflichtet sich, dafür Sorge zu tragen, dass keine durch seine Mitarbeitenden mitgebrachten Geräte an die Netze des Auftraggebers angeschlossen werden. Besteht die Notwendigkeit der Arbeit in IT-Infrastrukturen des Auftraggebers, so ist beim Ansprechpartner des Auftraggebers die Bereitstellung von durch den Auftraggeber administrierten Geräte zu beantragen und nur nach dessen Einwilligung gestattet.

4.2.2 Zutritts-, Zugangs- und Zugriffsrechte

1. Berechtigungen für den Zutritt zu Gebäuden oder Räumlichkeiten, den Zugang und/oder Zugriff auf Informationswerte oder Informationssysteme des Auftraggebers werden auf Antrag nach dem Grundsatz „Kenntnis nur, wenn nötig" durch den Auftraggeber vergeben und entsprechend eingeschränkt.
2. Die Einrichtung von Berechtigungen erfolgt durch die Mitarbeitenden des Auftraggebers. Sie werden personalisiert vergeben.
3. Jeder Mitarbeitende des Auftragnehmers, der entfernten oder lokalen Zugriff auf Informationswerte des Auftraggebers im Rahmen der Leistungserbringung benötigt, hat personenbezogene Informationen (mind. Vorname, Nachname, Mailadresse) zu seiner Identität bereitzustellen, damit durch den Auftraggeber entsprechende personalisierte Zugänge bereitgestellt werden können. Eine Weitergabe von personalisierten Benutzerkennungen und Kennwörtern ist untersagt.

4. Der Auftragnehmer stellt sicher, dass die seinen Mitarbeitenden bereitgestellten Zugänge nicht missbraucht werden und er seine Mitarbeitenden mit den entsprechenden Sicherheitsvorgaben des Auftraggebers bekannt gemacht hat.
5. Der Auftraggeber weist hiermit den Auftragnehmer darauf hin, dass Zutritte, Zugänge und Zugriffe protokolliert werden.
6. Die Verwendung der vergebenen Berechtigungen ist nur im Sinne und zum Zweck der Auftragserfüllung gestattet. Jegliche private Nutzung ist untersagt.

4.2.3 Fernzugriff zur Leistungserbringung (mobiles Arbeiten)

1. Die Zulassung und Art der Einrichtung eines Fernzuganges (Mobiles Arbeiten, Wartungszugänge) zur IT-Infrastruktur des Auftraggebers wird ausschließlich durch den Auftraggeber vorgegeben.
2. Grundsätzlich wird dem Auftragnehmer und seinen Mitarbeitenden – sofern für die Leistungserbringung notwendig - für das mobile Arbeiten ein vom Auftraggeber administriertes Gerät bereitgestellt, über welches er per VPN des Auftraggebers mit kontrollierter Berechtigungsstruktur auf IT-Infrastrukturen des Auftraggebers zugreifen kann.
3. Sollte darüber hinaus zur Leistungserbringung gewünscht sein, Fernzugänge mit Geräten des Auftragnehmers zu nutzen, so ist dies nur nach Prüfung und Einwilligung durch den Informationssicherheitsbeauftragten des Auftraggebers zulässig.
4. Wenn zur IT-Infrastruktur des Auftraggebers Verbindungen via Fernzugang hergestellt werden, muss der Auftragnehmer sicherstellen, dass über den entsprechenden Endpunkt beim Auftragnehmer kein unkontrollierter Zugriff durch Dritte auf die IT-Infrastrukturen und Daten des Auftraggebers ermöglicht wird und die Vertraulichkeit, Verfügbarkeit und Integrität der Assets, Services und Informationswerte des Auftraggebers gewährleistet sind. Dies beinhaltet auch die nachträgliche Verwendung von Informationen des Auftraggebers, von denen der Auftragnehmer und seine Mitarbeitenden während eines Fernzugriffes Kenntnis erlangt hat.
5. Für den Austausch von Information mit dem Auftraggeber, so z. B. in Projekten, vereinbart der Auftraggeber mit dem Auftragnehmer Sicherheitsmaßnahmen, die dem Schutzbedarf der bearbeiteten Informationen angemessen sind.
6. Der Auftragnehmer ist für alle Aktionen der Benutzerkonten mit Fernzugangsfunktion auf Systeme des Auftraggebers verantwortlich und dokumentiert nachvollziehbar Ort, Datum, Zeit, Arbeitskraft und die durchgeführten Tätigkeiten.
7. Im Rahmen der Leistungserbringung dürfen durch den Auftragnehmer weder technisches Equipment des Auftraggebers ins Ausland mitgeführt noch von dort auf die Systeme des Auftraggebers zugegriffen werden. Bei Bedarf kann die Mitnahme in und der Zugriff aus einem Mitgliedsstaat der Europäischen Union geprüft und ggf. durch die Exportkontrollabteilung des Auftraggebers freigegeben werden.

4.2.4 Übertragen von Informationen auf IT-Infrastrukturen des Auftragnehmers

1. Werden zur Erfüllung des Auftrages Informationen auf Systeme des Auftragnehmers oder seiner Mitarbeitenden übertragen und/oder werden Informationen des Auftraggebers auf IT-Infrastrukturen des Auftragnehmers verarbeitet, hat der Auftragnehmer, dem Schutzbedarf der Informationen des Auftraggebers entsprechend, für angemessene technische und/oder organisatorische Maßnahmen in Absprache mit dem Auftraggeber Sorge zu tragen. Entsprechende Sicherheitskonzepte bedürfen der Einwilligung des Auftraggebers und sind diesem auf Anforderung vorzulegen.
2. Der Auftragnehmer muss sicherstellen, dass Informationen des Auftraggebers auf dem Transportweg gegen Verlust, Veränderung und/oder Kenntnisnahme durch Unberechtigte nach Stand der Technik geschützt sind.
3. Der Auftragnehmer muss angemessene Vorkehrungen zur physischen Sicherheit und zum Zutrittsschutz zu seinen Bereichen mit Informationswerten des Auftraggebers treffen. Entsprechende Sicherheitskonzepte sind dem Auftraggeber auf Anforderung bereitzustellen.

4. Werden IT-Systeme oder Komponenten des Auftragnehmers, auf denen Informationen des Auftraggebers gespeichert sind, zur Reparatur gegeben oder einer Entsorgung zugeführt, muss gewährleistet sein, dass diese Daten nicht für Unberechtigte lesbar oder anderweitig auswertbar sind. Entsprechende Vernichtungsnachweise sind dem Auftraggeber auf Anforderung bereitzustellen. Der Stand der Technik nach Vorgaben des BSI zur sicheren Vernichtung von Informationen ist nachweislich anzuwenden.

4.2.5 Verschlüsselung

1. Sensible Informationen des Auftraggebers dürfen außerhalb der IT-Infrastrukturen des Auftraggebers nur verschlüsselt (via S/MIME oder vergleichbare Verfahren) weitergegeben werden. Der Auftraggeber weist seine Mitarbeitenden an, die entsprechenden Vorgaben des Auftraggebers zu beachten.

2. Eventuelle zur Ver- und Entschlüsselung von Informationen des Auftraggebers notwendige Passwörter, PINs oder Schlüssel sind über einen separaten Kommunikationsweg zu versenden. Der Auftragnehmer weist seine Mitarbeitenden an, die entsprechenden Vorgaben des Auftraggebers zu beachten.

4.2.6 Anforderungen an Softwareentwicklungsprozesse beim Auftragnehmer

Die Softwareentwicklungsprozesse des Auftragnehmers müssen so ausgelegt sein, dass der Sicherheit der zu entwickelnden Software, dem Schutzbedarf angemessen, in allen wichtigen Entwicklungsphasen Rechnung getragen wird und die Prozesse sich an den allgemein anerkannten Industriestandards orientieren. Hier sind die mit dem Auftraggeber im Vorfeld vereinbarten Sicherheitsmaßnahmen nach dessen Einwilligung umzusetzen. Entsprechende Sicherheitskonzepte sind dem Auftraggeber bei Bedarf vorzulegen.

Insbesondere müssen folgende Aspekte berücksichtigt werden:
1. Vorhandene Standards der sicheren Softwarearchitektur und Programmierung sind anzuwenden.
2. Die Anwendung entsprechender Standards ist zu dokumentieren.
3. Secure-Code-Reviews als Teil der Qualitätssicherung und Zurverfügungstellung der Ergebnisse sind ggf. nach Vorgabe des Auftraggebers zwischen Auftraggeber und Auftragnehmer zu vereinbaren und umzusetzen.
4. Die angemessene Konfiguration, Dokumentation und Wartung von Open Source Komponenten und Sicherheitsüberprüfungen – inkl. Nachweisführung - des eingesetzten Codes sind durch den Auftragnehmer sicherzustellen. Insbesondere ist eine Prüfung auf Schadsoftware durch den Auftragnehmer vorzunehmen.

4.2.7 Auditierungen

1. Der Auftragnehmer stimmt zu, dass der Auftraggeber oder ein durch den Auftraggeber beauftragter Dritter den Auftragnehmer, mit Bezug zum Auftrag, zu den Inhalten der Sicherheitsvereinbarung auditiert. Die Audits werden u. a. auf der Grundlage der von dem Auftragnehmer bei Bedarf dem Auftraggeber zur Verfügung gestellten Dokumentationen durchgeführt.
2. Der genaue Umfang, die Dauer und die Organisation der Audits werden einvernehmlich zwischen Auftragnehmer und Auftraggeber vereinbart.
3. Wird der Auftragnehmer aufgefordert, eine Selbstauskunft zur Sicherheit zu tätigen, ist hierfür die entsprechende Dokumentenvorlage des Auftraggebers zu nutzen und innerhalb eines mit dem Auftraggeber zu vereinbarenden Zeitraums zu übergeben.
4. Abweichungen von den vereinbarten Sicherheitsanforderungen sind dem Auftraggeber unverzüglich zu melden.
5. Der Auftraggeber bestätigt in mit dem Auftraggeber vereinbarten zeitlichen Abständen die Einhaltung der Vorgaben dieser Sicherheitsvereinbarung.

6. Auf Anforderung des Auftraggebers legt der Auftragnehmer Informationen über vorhandene Zertifizierungen zur Informationssicherheit dem Auftraggeber zur Einsicht vor.

4.2.8 Geheimschutzrelevante Aufträge

Bearbeitet der Auftragnehmer im Rahmen der Leistungserbringung Verschlusssachen (VS), so gelten die mit dem Auftraggeber zusätzlich vereinbarten Vorgaben. Diese ergänzen die Vereinbarungen im vorliegenden Dokument.

5. Maßnahmen NACH Erbringung einer Dienstleistung

5.1 Entzug von Zutritts-, Zugangs- und Zugriffsberechtigungen

Wird der Vertrag beendet und so weit nicht vertraglich anderweitig geregelt, hat der Auftragnehmer mit Vertragsbeendigung sicherzustellen, dass jegliche Gerätschaft, Software oder Information in elektronischer Form oder Papierform an den Auftraggeber zurückgegeben werden. Weiterhin gelten auch hier die Vorgaben von 4.2.4 Pkt.4.