1. Ziel und Zweck des Dokumentes

In dieser Richtlinie werden Regeln für den Umgang mit Informationen und der **Informationssicherheit** definiert, die Lieferanten, Werkunternehmer und Dienstleister sowie sonstige Dritte (nachfolgend Auftragnehmer genannt), die Tätigkeiten für **IT-HAUS GmbH** ausführen und dabei mit Informationswerten von **IT-HAUS GmbH** in Berührung kommen oder solche verarbeiten oder schützen.
Ziel dieser Richtlinie ist daher die Regelung der Pflichten des Auftragnehmers für den Umgang und Gebrauch von Informationswerten der **IT-HAUS GmbH,** um den Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie der Rechte und Interessen der **IT-HAUS GmbH** zu gewährleisten.

2. Zuständigkeiten

Für diese Richtlinie ist der „Informationssicherheitsbeauftragte“ (ISB) in Abstimmung mit der Geschäftsführung zuständig.

3. Geltungsbereich

Die Richtlinie richtet sich an die Geschäftsleitung des Auftragnehmers, deren Mitarbeiter sowie deren Erfüllungs-/Verrichtungsgehilfen.

4. Anforderungen an die IT- und Informationssicherheit

4.1. Wahrung von Vertraulichkeit von Informationen/Betriebsgeheimnissen

IT-HAUS GmbH arbeitet ausschließlich mit Auftragnehmern zusammen, welche sich zur Wahrung von Vertraulichkeit von Informationen und Betriebsgeheimnissen im Rahmen einer Geheimhaltungsverpflichtung oder einer Geheimhaltungsvereinbarung verpflichtet haben. In Einzelfällen, wenn die übergebenen Informationen einem gesteigerten Sicherheitsbedürfnis unterfallen, können darüber hinaus besondere Maßnahmen von Auftragnehmern gefordert werden, um dem gesteigerten Sicherheitsbedürfnis Rechnung zu tragen.

4.2. Technische und organisatorische Maßnahmen der Informations- und IT-Sicherheit

Die Vertraulichkeit und Integrität von schutzbedürftigen Daten sowie deren Verfügbarkeit bzw. die Aufrechterhaltung des Betriebs und wichtiger Geschäftsprozesse sind des Weiteren durch wirksame und angemessene technische und organisatorische Maßnahmen sicherzustellen.

4.2.1. Management der Informationssicherheit

IT- und Informationssicherheit genießen bei **IT-HAUS GmbH** einen sehr hohen Stellenwert. Der Auftraggeber setzt voraus, dass der Auftragnehmer in seinem Unternehmen geeignete Prozesse zur Gewährleistung der IT- und Informationssicherheit im Rahmen der Leistungserbringung etabliert und dieses während der gesamten Laufzeit aufrecht hält. Beispielsweise geschieht dies in Form eines angemessenen Informationssicherheitsmanagementsystems (ISMS) oder durch gleichwertige, geeignete Prozesse zur Gewährleistung der Informationssicherheit im Rahmen der Leistungserbringung. Die Informationssi-

cherheitsprozesse des Auftragnehmers entsprechen mindestens den nachfolgend beschriebenen Informationssicherheitsanforderungen und orientieren sich an der ISO/IEC 27001 oder einer gleichwertigen Anforderung.

4.2.2. Berücksichtigung einschlägiger Gesetze und Normen für die Leistungserbringung

Der Auftragnehmer beachtet die einschlägigen datenschutzrechtlichen Vorschriften. Sofern anwendbar, erwartet die **IT-HAUS GmbH** überdies die Einhaltung von Anforderungen, die sich aus weiteren einschlägigen Gesetzen und Normen für die Leistungserbringung des Geschäftspartners ergeben, wie z. B. NIS2.

4.2.3. Ansprechpartner zur Informationssicherheit

Der Auftragnehmer muss **IT-HAUS GmbH** für alle Aspekte rund um Informationssicherheit einen sachkundigen Ansprechpartner (z.B. Informationssicherheitsbeauftragten, IT-Sicherheitsmanager) benennen, der gegenüber dem Auftraggeber in allen Fragen des Managements der Informationssicherheit auskunftsfähig und auskunftsberechtigt ist. Auf Anforderung hin gibt der Ansprechpartner des Auftragnehmer Auskunft zum Stand der IT- und Informationssicherheit (z. B. mittels Fragebogen zur Informationssicherheit oder durch Nachweis eines nach ISO 27001 zertifiziertem ISMS mit einem Scope, welcher die Dienstleistungen für den Auftraggeber umfasst).

4.2.4. Qualifiziertes Personal

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen und Anforderungen zur Informationssicherheit vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet. Der Auftragnehmer weist dies **IT-HAUS GmbH** auf Anfrage nach.

4.2.5. Verpflichtung Unterauftragnehmer

Der Auftragnehmer gewährleistet, dass seine zur Leistungserbringung eingesetzten Unterauftragnehmer und, so weit vereinbart, deren Subunternehmer die Anforderungen aus dieser Richtlinie, die der ISO/IEC 27001 oder solche einer vergleichbaren Norm erfüllen. Er stellt entsprechende Nachweise auf Anforderung von **IT-HAUS GmbH** zur Verfügung.

4.2.6. Allgemeine Sicherheitsvorgaben zum Zugang und Zugriff auf IT-Systeme

Der Auftragnehmer ist verpflichtet, über ein Verfahren zur regelmäßigen Überprüfung von Zugriffsrechten zu verfügen, um sicherzustellen, dass ausschließlich autorisierte Personen auf IT-Systeme der **IT-HAUS GmbH** zugreifen können. Bei jedem Zugriff auf IT-Systeme der **IT-HAUS GmbH** muss der Auftragnehmer alle Sicherheitsmaßnahmen und Bedingungen einhalten (und sicherstellen, dass sein Personal diese einhält), die zur Leistungserbringung erforderlich sind. Die **IT-HAUS GmbH** ermächtigt den Auftragnehmer nur dann zum Zugriff auf die IT-Systeme der **IT-HAUS GmbH**, wenn dies vereinbart ist und ausschließlich nur im erforderlichen Rahmen der Leistungserbringung.
Die Mitnahme von Arbeitsergebnissen oder IT-Systemen der **IT-HAUS GmbH** aus den Geschäftsräumen der **IT-HAUS GmbH** ist nur im Rahmen der vereinbarten Leistungserbringung zulässig und bedarf der vorherigen schriftlichen Genehmigung der **IT-HAUS GmbH**.

Die hinterlegten Authentifizierungsinformationen (Kennungen und Passwörter) auf datenverarbeitenden Systemen der **IT-HAUS GmbH** müssen personenscharf verwandt werden. Eine Weitergabe oder Offenlegung für Dritte ist untersagt.
Der Auftragnehmer stellt sicher, dass nur die Mitarbeiter Zugang zu Informationen der **IT-HAUS GmbH** erhalten, die auch an der Lieferleistung mitwirken. Der Zugang und Zugriff auf die IT-Systeme der **IT-HAUS GmbH** darf nur für die vereinbarten Zwecke und Aufgaben erfolgen.
Der Auftragnehmer setzt für die eigenen Systeme, auf denen Informationen der **IT-HAUS GmbH** verarbeitet werden, ein nach Stand der Technik sicheres Anmeldeverfahren (z. B. Multi-Faktor-Authentifizierung oder Nutzung starker Kennwörter) für den Zugang zu diesen Systemen und Anwendungen ein.
Der Auftragnehmer trifft alle notwendigen Vorkehrungen, um die Einschleusung eines Computervirus in die die Software-/ & IT-Systeme der **IT-HAUS GmbH** zu vermeiden, und ergreift geeignete Maßnahmen, wenn er das Vorhandensein eines solchen Virus bemerkt. Der Auftragnehmer verpflichtet sich, alle Vorkehrungen und Maßnahmen zu treffen, die von einem sorgfältigen Vertragspartner zu erwarten sind, um sicherzustellen, dass er keinen Sicherheitsvorfall in Bezug auf seine Lieferungen und/oder Leistungen und/oder im Informationssystem der **IT-HAUS GmbH**, auf das der Auftragnehmer Zugriff hat, erzeugen oder verursachen wird, oder dies zu begünstigen.

4.3. Meldung Sicherheitsvorfälle

Für den Fall, dass dem Auftragnehmer ein rechtswidriger oder unbefugter Zugriff und/oder eine Nutzung von Daten und/oder IT-Systemen der **IT-HAUS GmbH** oder des Auftragnehmers bekannt wird oder ein solches Ereignis vermutet, verpflichtet sich der Auftragnehmer, der **IT-HAUS GmbH** einen solchen (vermuteten) Sicherheitsvorfall schriftlich zu melden, sobald er davon Kenntnis erlangt und/oder er von einer für ihn direkt oder indirekt zuständigen Behörde hierüber benachrichtigt wird.

In einem solchen Fall ergreift der Auftragnehmer alle geeigneten Maßnahmen, die ein sorgfältiger Auftragnehmer zum Schutz seiner Daten und/oder seiner IT-Systeme sowie Daten und/oder IT-Systeme der **IT-HAUS GmbH** ergreifen würde, einschließlich, aber nicht beschränkt auf die Unterbrechung der Verbindung und/oder die Sperrung des Zugangs. In keinem Fall haftet die **IT-HAUS GmbH** für die Folgen einer Verschlechterung der Beschaffenheit der Lieferungen und/oder Leistungen infolge der in diesem Fall getroffenen Maßnahmen.

Darüber hinaus muss der Auftragnehmer im Falle eines unerlaubten oder unbefugten Zugriffs und/oder Nutzung der Informationssystems / IT-Systems der **IT-HAUS GmbH** und/oder bei Verdacht auf ein solches Ereignis und/oder im Falle eines sonstigen Sicherheitsvorfalls, den **IT-HAUS GmbH** Service-Desk per E-Mail servicedesk@it-haus.com oder telefonisch +49 6502 9208 110 benachrichtigen, sobald er davon Kenntnis erlangt, spätestens jedoch einen (1) Kalendertag nach einem (vermuteten) Sicherheitsvorfall.