Verpflichtungserklärung zur Erfüllung der Informationssicherheitsrichtlinie für Dienstleister

Version	Datum	Bearbeitungsart / Betroffene Abschnitte	Bearbeiter
1.0	01.04.2018	Freigabe erste Version durch PKM	J. Holtmannspötter
1.1	12.04.2018	Einarbeitung redaktioneller Änderungen von REV	J. Holtmannspötter
1.2	30.04.2018	Einarbeitung redaktioneller Änderungen von PKM	J. Holtmannspötter
1.3a	16.1.2020	Ergänzungen nach ISMS Audit	J. Holtmannspötter

Verpflichtungserklärung zur Erfüllung der Informationssicherheitsrichtlinie für Dienstleister

Auftragnehmer, die im Rahmen der Vertragsdurchführung, Zugriff oder Zugang auf firmeneigene Informationen sowie Netze und Systeme erhalten, verpflichten sich einmalig, die Regelungen dieser Richtlinie auf unbestimmte Zeit einzuhalten.

Erbringung von Dienstleistungen:

Der Auftragnehmer erhält zur Erfüllung seiner Aufträge die Möglichkeit sich am Kommunikationsnetz des Auftraggebers anzumelden.
Er ist lediglich befugt, die zur Erfüllung seiner Aufträge benötigten Systeme zu nutzen.

Der Auftraggeber behält sich das Recht vor, Mitarbeiter des Auftragnehmers auf ausreichende Qualifikation hin zu überprüfen und im Zweifel die Ablösung des Personals zu verlangen. Erst nach einer Einweisung durch einen Mitarbeiter des Auftraggebers sind Mitarbeiter des Auftragnehmers dazu berechtigt, Tätigkeiten mit Zugriff auf Informationen und informationsverarbeitende Einrichtungen durchzuführen.

Der Auftraggeber behält sich weiterhin das Recht vor, den Auftragnehmer im Rahmen von Audits zu überprüfen, um sicher zu stellen, dass ausgegliederte Prozesse oder extern vergebene Entwicklungstätigkeiten ordnungsgemäß durchgeführt werden. Dafür ist dem Auftraggeber nach Abstimmung Zugriff und Zugang zu den Daten und Einrichtungen des Auftragnehmers zu gewähren.

Eine Beauftragung von Nachunternehmern ist nur nach vorheriger Nennung und schriftlicher Zustimmung durch den Auftraggeber gestattet.

Zur Erfüllung der Anforderungen der informationstechnischen Sicherheit verpflichtet sich der Auftragnehmer mindestens zur Einhaltung der folgenden Sicherheitsmaßnahmen:

1. Ausschließlicher Zutritt zu den, durch den Auftraggeber freigegebenen Bereichen.

2. Der Auftraggeber behält sich das Recht vor, die Tätigkeiten des Auftragnehmers Vor-Ort, insbesondere in Bereichen mit kritischer Infrastruktur, durch eigenes Personal zu überwachen.

3. Ausschließliche Verwendung der durch den Auftraggeber freigegebenen oder lizenzierten Hard- und Software.

4. Ausschließliche Nutzung der durch den Auftraggeber freigegebenen Kommunikationsverbindungen.

5. Nutzung von Hardware, Software und Informationen ausschließlich zur Erfüllung der vereinbarten Aufgaben.

6. Ausschließliche Verwendung von Datenträgern, die auf Schadprogramme geprüft und durch den Auftraggeber freigegeben wurden.

7. Nach Beendigung des Auftrages hat der Auftragnehmer sämtliche Werte des Auftraggebers unverzüglich diesem auszuhändigen und nach Ablauf der Gewährleistung ggf. noch vorhandene Daten auf seinen Systemen zu vernichten.

8. Als vertraulich klassifizierte und gekennzeichnete Werte des Auftraggebers dürfen nicht an Dritte weitergegeben werde, auch nicht nach Auftragsende.

9. Nutzung der im Rahmen der vereinbarten Leistung zugewiesenen Rechte.

10. Einhaltung der IT-Benutzerrichtlinie KR07 bei Erbringung von Dienstleistungen in unserem Kommunikationsnetzwerk. Diese wird dem Auftragnehmer durch Mitarbeiter des Auftraggebers auf Anforderung zur Verfügung gestellt.

11. Unverzügliche Meldung von erkannten Sicherheitslücken an den IT-Sicherheitsbeauftragen des Auftraggebers. [Jürgen Holtmannspötter, 0209 / 708 656]

12. Alle Daten und Informationen werden ausschließlich innerhalb der EU verarbeitet und gespeichert. Sofern Daten außerhalb der EU verarbeitet oder gespeichert werden ist sicherzustellen, dass ein angemessener Schutz vertraglich gewährleistet ist.

13. Bei Übertragung von vertraulichen oder sicherheitsrelevanten Daten über öffentliche Netze, sind die übertragenen Daten zu verschlüsseln.

Lieferung von Software:

Bei der Lieferung von Software, Programmen, Quellcode und Softwarelizenzen ist dem Auftraggeber ein Nachweis zu erbringen, dass diese vom Auftragnehmer geprüft und frei von Schadsoftware sind.

Der Auftragnehmer muss bei der Auslieferung dem Auftraggeber mindestens über:

- Ausgelieferter Versionsstand
- Aktuell höchster verfügbarer Versionsstand
- Status der Software (LTS, freigegeben, Beta-Version usw.)
- Hardware-/Systemkompatibilität
- Freigabe am
- Freigabe durch

schriftlich informieren.

Bei der Lieferung von Software hat der Auftragnehmer den Auftraggeber darüber zu informieren, ob ein Standardpasswort eingerichtet ist und wenn ja, wie dieses durch ein individuelles Passwort ersetzt werden kann.

Alle voreingestellten Kommunikationsprozesse über das Internet (http, https, ftp usw.) sind entweder durch den Auftragnehmer zu deaktivieren oder falls dies nicht möglich ist, muss er den Auftraggeber darüber schriftlich informieren, dass diese existieren.

Alle dem Auftragnehmer bekannten Sicherheitslücken sind vor der Auslieferung zu beheben und nach der Auslieferung erkannte Sicherheitslücken dem IT-Sicherheitsbeauftragten des Auftraggebers unverzüglich schriftlich mitzuteilen.

Lieferung von Hardware:

Bei der Lieferung von Hardwarekomponenten hat der Auftragnehmer den Auftraggeber darüber zu informieren, ob ein Standardpasswort eingerichtet ist und wenn ja, wie dieses durch ein individuelles Passwort ersetzt werden kann.

Alle voreingestellten Kommunikationsprozesse über das Internet (http, https, ftp usw.) sind entweder durch den Auftragnehmer zu deaktivieren oder falls dies nicht möglich ist, muss er den Auftraggeber darüber schriftlich informieren, dass diese existieren.

Alle dem Auftragnehmer bekannten Sicherheitslücken sind vor der Auslieferung zu beheben und nach der Auslieferung erkannte Sicherheitslücken dem IT-Sicherheitsbeauftragten des Auftraggebers unverzüglich schriftlich mitzuteilen.

Vertraulichkeitsvereinbarung

Vertrauliche Informationen im Sinne dieser Vereinbarung sind:

- Alle mündlichen oder schriftlichen Informationen und Materialien die der Auftragnehmer direkt oder indirekt vom Auftraggeber zur Abwicklung des Auftrages erhält und als vertraulich gekennzeichnet sind oder deren Vertraulichkeit sich aus ihrem Gegenstand oder sonstigen Umständen ergibt.

- Die beauftragten Leistungen und Arbeitsergebnisse.

Der Auftragnehmer verpflichtet sich, alle ihm direkt oder indirekt zur Kenntnis erlangten vertraulichen Informationen strikt vertraulich zu behandeln und nicht ohne vorherige schriftliche Zustimmung des Auftraggebers an Dritte weiterzugeben, zu verwerten oder zu verwenden.

Die Verpflichtung zur Vertraulichkeit gilt nicht, wenn eine Verpflichtung zur Offenlegung der vertraulichen Information durch Beschluss eines Gerichts, Anordnung einer Behörde oder ein Gesetz besteht.

Der Auftragnehmer wird alle technischen und organisatorischen Maßnahmen treffen, um die Vertraulichkeit sicherzustellen. Vertrauliche Informationen werden nur an die Mitarbeiter oder Dritte weitergegeben, die sie aufgrund ihrer Tätigkeit erhalten müssen. Der Auftragnehmer unterweist die zum Einsatz kommenden Personen gemäß dieser Informationssicherheitsrichtlinie.

Die Pflicht zur absoluten Vertraulichkeit besteht auch nach Beendigung der Zusammenarbeit an. Auf Verlangen sind ausgehändigte Unterlagen einschließlich aller davon angefertigten Kopien sowie Arbeitsunterlagen und -Materialien zurückzugeben.

Der Auftragnehmer haftet für alle Schäden im Rahmen der gesetzlichen Vorgaben, die dem Auftraggeber durch Verletzung dieser vertraglichen Pflichten entstehen.

Ein Verstoß gegen die Bestimmungen der Richtlinie kann zum sofortigen Entzug der Zugangs- und Zugriffsberechtigungen führen.

Die Vertraulichkeitsverpflichtung und sonstigen Regelungen dieser Richtlinie gelten auch für die Rechtsnachfolger der Parteien. Änderungen und Ergänzungen dieser Vereinbarungen bedürfen der Schriftform.

_____

Firmenstempel, Datum und Unterschrift