Allgemeine Geschäftsbedingungen des Kantons Solothurn über die Informationssicherheit und den Datenschutz bei der Erbringung von Informatikdienstleistungen (AGB ISDS)

1. Allgemeine Bestimmungen

1.1. Zweck

Diese AGB bezwecken den Schutz der Persönlichkeitsrechte der Personen, deren Daten bearbeitet werden, und die Gewährleistung der Informationssicherheit bei der Erbringung von Informatikdienstleistungen durch Dritte für den Kanton Solothurn.

1.2. Begriffe

a) Leistungserbringerin: Natürliche und juristische Personen sowie öffentlich-rechtliche Institutionen, die für den Kanton Solothurn Informatikdienstleistungen erbringen.

b) Leistungsbezüger: Der Kanton Solothurn, vertreten durch seine Organe oder Dienststellen wie Regierungsrat, Departemente, Staatskanzlei, Organisationseinheiten, Ämter, Betriebe und Gerichte, der die Leistungserbringerin mit der Erbringung von Informatikdienstleistungen beauftragt.

c) Informatikdienstleistungen: Leistungen im Bereich der Informatik oder Telekommunikation, insbesondere Kommunikationsdienste, Rechenzentrumsdienste, Aufbau und Betrieb von Büroinformationssystemen, Anwendungsentwicklung und -wartung, sowie jegliche Datenverarbeitung.

1.3. Gegenstand und Geltung

[1] Diese AGB gelten für die Informatikdienstleistungen, welche die Leistungserbringerin für die Leistungsbezüger erbringt und die die Bearbeitung von Daten des Leistungsbezügers beinhalten sowie für die damit verbundenen Geschäftsprozesse der Leistungserbringerin oder des Leistungserbringers.

[2] Diese AGB gelten auch für Subunternehmer oder -unternehmerinnen, Beauftragte, Hilfspersonen und Mitarbeitende der Leistungserbringerin, die im Zusammenhang mit Daten, Systemen und Prozessen des Leistungsbezügers tätig werden.

1.4. Verhältnis zur vertraglichen Regelung

[1] Die vorliegenden AGB sind Teil eines Vertrags zwischen Leistungserbringerin und Leistungsbezüger. Sieht dieser vor, dass weitere AGB zur Anwendung kommen, namentlich die «AGB für IKT-Leistungen» der «Digitalen Verwaltung Schweiz DVS» (AGB DVS), treten die Bestimmungen der vorliegenden AGB an die Stelle der Informationssicherheits- und Datenschutzbestimmungen der weiteren AGB.

[2] Im Übrigen gehen die Bestimmungen der anderen Vertragsbestandteile den vorliegenden AGB vor.

2. Rechte und Pflichten der Parteien

2.1. Verantwortung und rechtliche Verfügungsmacht über die Information

[1] Der Leistungsbezüger bleibt für die Bearbeitung der Informationen verantwortlich. Die Leistungserbringerin darf die Informationen ausschliesslich im Rahmen der vertraglichen Vereinbarung bearbeiten. Die Leistungserbringerin hat weiteren Weisungen des Leistungsbezügers in Bezug auf die Informationsbearbeitung Folge zu leisten.

[2] Der Leistungsbezüger behält vollumfänglich die rechtliche Verfügungsmacht über die in seinem Auftrag bearbeiteten Informationen. Er kann der Leistungserbringerin ungeachtet der konkreten vertraglichen Situation jederzeit den Zugriff auf die bearbeiteten Informationen

untersagen, diese unentgeltlich im vereinbarten Format herausverlangen oder die Leistungserbringerin auffordern, die im Rahmen des Auftrags bearbeiteten Informationen zu vernichten.

2.2. Verhältnismässigkeit und Zweckbindung

[1] Die Leistungserbringerin darf ausschliesslich jenen Mitarbeitenden den Zugriff auf die im Rahmen des Auftrags bearbeiteten Informationen ermöglichen, die diese zur Auftragserfüllung tatsächlich benötigen.
[2] Die Bearbeitung der Informationen darf ausschliesslich zum vertraglich festgelegten Zweck erfolgen. Jede andere Bearbeitung, insbesondere jede Bearbeitung zu eigenen Zwecken, ist ausdrücklich untersagt.

2.3. Informationspflichten

[1] Die Leistungserbringerin informiert und dokumentiert den Leistungsbezüger auf Anfrage über die Methoden und Prozesse, die sie zur Erbringung ihrer vertraglichen Leistungen einsetzt und die für die Einhaltung von Informationssicherheit und den Datenschutz (ISDS) gemäss Anhang 1 relevant sind. Der Leistungsbezüger kann die entsprechenden Unterlagen vor Ort einsehen und sich die betrieblichen Abläufe vorführen lassen.
[2] Die Leistungserbringerin informiert den Leistungsbezüger unverzüglich über aussergewöhnliche Vorfälle, die die Daten, Systeme und Prozesse des Leistungsbezügers betreffen, namentlich über bedeutende ISDS-Verletzungen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verstösse gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmässigkeiten beim Umgang mit Daten des Leistungsbezügers.
[3] Die Leistungserbringerin meldet dem Leistungsbezüger unverzüglich alle Verstösse gegen Vorschriften zum Schutz der Informationen des Leistungsbezügers oder gegen weitere vertragliche Bestimmungen. Die Meldepflicht ist verursacherunabhängig. Sie besteht insbesondere im Falle des Verlustes, der unrechtmässigen Übermittlung oder unrechtmässigen Kenntnisnahme von Daten.
[4] Sollte die Leistungserbringerin aufgrund einer richterlichen Verfügung verpflichtet werden, Behörden Zugang zu Systemen und Informationen des Leistungsbezügers zu verschaffen, informiert sie den Leistungsbezüger unverzüglich.

2.4. Einhaltung des ISDS-Grundschutzes

Die Leistungserbringerin stellt den ISDS-Grundschutz gemäss Anhang 1 zu den vorliegenden AGB sicher. Leistungsspezifische Präzisierungen des ISDS-Grundschutzes sind schriftlich zu vereinbaren.

2.5. Penetrationtests und Sicherheitsaudits

Die Leistungserbringerin ist bereit, die Bedingungen des Bereiches Penetrationstests und Sicherheitsaudits gemäss Anhang 2 zu den vorliegenden AGB zu akzeptieren. Leistungsspezifische Präzisierungen betreffend Penetrationstests und Sicherheitsaudits sind schriftlich zu vereinbaren.

2.6. Beizug von Dritten

Die Leistungserbringerin darf für die Verarbeitung oder Nutzung von Daten des Leistungsbezügers Dritte nur einbeziehen, wenn folgende Bedingungen kumulativ eingehalten werden:

1. Der Leistungsbezüger erteilt seine schriftliche Zustimmung.
2. Die Leistungserbringerin verpflichtet die beigezogenen Dritten (Ziff. 1.3 Abs. 2 der vorliegenden AGB) schriftlich zur Einhaltung der Vertraulichkeit (Ziff. 2.7) und schreibt die Einhaltung der gesetzlichen und vertraglichen ISDS-Bestimmungen vor. Sie informiert diese Dritten über die gesetzlichen und vertraglichen ISDS-Bestimmungen.
3. Die Leistungserbringerin stellt vertraglich sicher, dass dem Leistungsbezüger Kontroll- und Überprüfungsrechte entsprechend Ziffer 2.10 beim Dritten zustehen. Dies umfasst auch das Recht des Leistungsbezügers, von der Leistungserbringerin Auskunft über den Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis zu erhalten.

2.7. Vertraulichkeit

[1] Die Leistungserbringerin und alle Personen, die mit der übertragenen Datenbearbeitung betraut sind oder die Zugang zu den im Rahmen des Auftrages bearbeiteten Informationen haben können, sind verpflichtet, über die Informationen und die Bearbeitung Verschwiegenheit zu wahren. Die Verschwiegenheitspflicht gilt auch innerhalb des Unternehmens der Leistungserbringerin ungeachtet der hierarchischen Positionen.
[2] Die Leistungserbringerin verpflichtet sich, alle Personen, die mit der übertragenen Datenbearbeitung betraut sind oder die Zugang zu den im Rahmen des Auftrages bearbeiteten Informationen haben können, vorgängig eine Erklärung unterzeichnen zu lassen, womit sie sich zu Verschwiegenheit im oben umschriebenen Sinn verpflichten und zur Kenntnis nehmen, dass vertragswidriges Bearbeiten strafbar ist. Die Leistungserbringerin legt dem Leistungsbezüger auf Verlangen die unterzeichneten Verpflichtungserklärungen vor.
[3] Die Geheimhaltungspflichten bestehen schon vor Vertragsabschluss und bleiben auch nach Beendigung des Vertragsverhältnisses bzw. nach Erfüllung der vereinbarten Leistung bestehen. Vorbehalten bleiben gesetzliche Auskunftspflichten.
[4] Die Leistungserbringerin darf die Tatsache und den wesentlichen Inhalt der Offertanfrage möglichen zu beauftragenden Dritten bekannt geben. Werbung und Publikation über projektspezifische Leistungen bedürfen der schriftlichen Zustimmung des Leistungsbezügers.

2.8. Sorgfalt bei Personalauswahl

Die Leistungserbringerin sorgt bei der Personalauswahl dafür, dass nur vertrauenswürdige Personen mit der vertraglichen Datenbearbeitung betraut werden (z.B. Strafregisterauszug, Betreibungsauskunft, Leumundszeugnis, langjährige Betriebszugehörigkeit etc.). Die Leistungserbringerin muss nachweisen, dass die Mitarbeitenden regelmässig in Bezug auf Datenschutz und Informationssicherheit geschult bzw. instruiert werden.

2.9. Weitergabe von Daten und Informationen

Die Leistungserbringerin darf Daten des Leistungsbezügers ohne anderslautende Ermächtigung nur für diesen verwenden und nur diesem bekannt geben. Begehren um Datenbekanntgabe von Privaten (ob von der Datenbearbeitung betroffen oder nicht), von anderen Behörden oder von anderen Stellen der kantonalen Verwaltung sind an den Leistungsbezüger weiterzuleiten, und diesem sind sämtliche für die Beantwortung des Gesuchs erforderlichen Angaben zu liefern.

2.10. Überwachung, Audits, Aufsicht und Kontrolle

[1] Der Leistungsbezüger hat das Recht, die Datenbearbeitungen jederzeit selber zu kontrollieren oder durch Dritte kontrollieren zu lassen. Die Audits erfolgen nach allgemein anerkannten Methoden durch interne oder externe, fachlich unabhängige und sachkundige Stellen. Die Leistungserbringerin ist nicht verpflichtet, mit Auditoren zusammenzuarbeiten, mit denen sie in einem Konkurrenzverhältnis steht.
[2] Die Leistungserbringerin liefert auf Anfrage alle Nachweise über die funktionierenden unternehmensinternen Kontrollen (z.B. IKS-Protokolle).
[3] Ist die Leistungserbringerin nach allgemein anerkannten Informationssicherheits- und Datenschutzstandards zertifiziert und wird sie in diesem Zusammenhang regelmässig auditiert, lässt sie dem Leistungsbezüger den Auditbericht zukommen, soweit dieser die Daten, Systeme und Prozesse des Leistungsbezügers betrifft.
[4] Die Leistungserbringerin untersteht, soweit Daten, Systeme und Prozesse der Leistungsbezüger betroffen sind, der Aufsicht des oder der Beauftragten für Information und Datenschutz des Kantons Solothurn (§ 32 ff. InfoDG). Der oder die Datenschutzbeauftragte des Kantons ist von Gesetzes wegen berechtigt, bei der Leistungserbringerin schriftlich oder mündlich Auskunft über Datenbearbeitungen einzuholen, Einsicht in alle Unterlagen zu nehmen, Besichtigungen durchzuführen und sich Bearbeitungen vorführen zu lassen. Die Leistungserbringerin unterstützt sie dabei unentgeltlich.
[5] Der Leistungsbezüger kann gegenüber der Leistungserbringerin und ihren Mitarbeitenden die Unterlassung oder die Änderung einer als rechts- oder vertragswidrig erkannten Bearbeitung anordnen.

2.11. Löschung von Daten und Rückgabe von Datenträgern

[1] Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Leistungsbezüger – spätestens mit Beendigung der Leistungsvereinbarung – hat die Leistungserbringerin sämtliche in ihrem Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, im vereinbarten Format dem Leistungsbezüger unentgeltlich auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht unentgeltlich zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
[2] Dokumentationen, die dem Nachweis der auftrags- und ordnungsmässigen Datenverarbeitung dienen, sind durch die Leistungserbringerin entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Sie kann sie zu ihrer Entlastung bei Vertragsende dem Leistungsbezüger übergeben.

2.11. Unterstützung durch den Leistungsbezüger

Der Leistungsbezüger unterstützt die Leistungserbringerin bei der Umsetzung ihrer Pflichten nach Massgabe der vorliegenden AGB.

3. Sanktionen

[1] Verletzt die Leistungserbringerin oder ein von ihr einbezogener Dritter vorstehende Geheimhaltungspflichten, so schuldet die Leistungserbringerin dem Leistungsbezüger eine Konventionalstrafe gemäss Ziffer 22.1 AGB DVS.
[2] Die Leistungserbringerin macht sich gemäss § 42 InfoDG strafbar, wenn sie ohne ausdrückliche Ermächtigung des Leistungsbezügers Personendaten für sich oder andere verwendet oder anderen bekannt gibt.

4. Vorzeitige Beendigung des Vertragsverhältnisses

Bei wiederholter schwerwiegender Pflichtverletzung steht der verletzten Partei das Recht zur sofortigen Vertragsauflösung zu. Das gleiche Recht steht dem Leistungsbezüger zu im Falle der Übernahme des Geschäfts der Leistungserbringerin durch einen Dritten oder im Falle des Konkurses oder der Geschäftsaufgabe der Leistungserbringerin.

5. Serverstandort

Die Leistungserbringerin verpflichtet sich, die Informationen ausschliesslich auf Servern zu bearbeiten, die sich physisch in der Schweiz befinden oder in einem Staat, welcher dem Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (Europarats-Konvention 108; SR 0.235.1) beigetreten ist.

6. Gerichtsstand und anwendbares Recht

[1] Auf dieses Vertragsverhältnis ist Schweizer Recht anwendbar.
[2] Für Streitigkeiten aus diesem Vertrag gilt der Gerichtsstand Solothurn oder ein anderer vertraglich vereinbarter Standort innerhalb der Schweiz.

Anhang 1: ISDS-Grundschutz

Die ISDS-Grundschutzmassnahmen sind für alle Datenbearbeitungen des Kantons umzusetzen. In der Folge werden diejenigen Bestimmungen des Grundschutzmoduls der ISDS-Wegleitung des kantonalen Amts für Informatik und Organisation wiedergegeben, die im Verantwortungsbereich der Leistungserbringenden liegen. Leistungsspezifische Präzisierungen sind im Vertrag zu regeln (Ziff. 2.4 der AGB ISDS).

1. Zutrittskontrolle (physisch)

Ziel: Verhinderung des Zutritts Unberechtigter zu Räumen, in denen Daten des Leistungsbezügers bearbeitet werden.

1.1. Organisatorische Massnahmen

1.1.1. Sensitive Räumlichkeiten (Bsp. Serverräume, Räume mit wichtigen Telekommunikationseinrichtungen, Räume für Backup-Kopien, Archive) müssen Sicherheitszonen zugewiesen werden.

1.1.2. Der Zutritt zu Informatikräumen und -mitteln ist mittels einer verbindlichen und nachvollziehbaren Zutrittsberechtigung zu regeln. Diese sollte sinnvoll abgestuft sein.

1.1.3. Es ist ein Schliessplan zu erarbeiten und zu dokumentieren, welcher Verantwortlichkeiten, Verwaltung, Vergabe und Rücknahme der Zutrittsmittel regelt.

1.2. Technische Massnahmen

1.2.1. Die Eingänge zu den Sicherheitszonen müssen über ein sicheres Schliess- und Zutrittssystem verfügen.

1.2.2. Schliess- und Zutrittssysteme müssen regelmässig auf ihre korrekte Funktionsweise überprüft werden.

1.2.3. Der Zutritt durch andere Gebäudeöffnungen ist durch raumsichernde Massnahmen, wie Fenstervergitterungen, Sicherheitsstoren usw. zu verhindern.

2. Zugangskontrolle

Ziel: Verhinderung der Nutzung von IT-Anlagen, -Diensten, -Anwendungen und Kommunikationseinrichtungen und Einsicht in Datenausgaben des Leistungsbezügers durch Unbefugte.

2.1. Organisatorische Massnahmen

2.1.1. Die Vergabe von Benutzerrechten muss verbindlich geregelt, dokumentiert und überwacht werden.

2.1.2. Accounts und Zugriffsrechte, die nicht mehr benötigt werden (z.B. wegen Austritts) oder die über längere Zeit nicht mehr benutzt worden sind, müssen gesperrt oder gelöscht werden.

2.1.3. In publikumszugänglichen Bereichen (z.B. Schalter, Sekretariaten) sind periphere Geräte wie Bildschirme und Drucker so zu platzieren, dass Unberechtigte keinen Einblick in die Daten haben.

2.2. Technische Massnahmen

2.2.1. Die Zugangsberechtigung auf Systeme erfolgt mit einer Benutzeridentifikation und einem sicheren Passwort. Für Passworte gilt:

- Passworte sind persönlich und geheim.
- Sie umfassen mindestens 12 Stellen und sind unter Verwendung von Buchstaben und Sonderzeichen oder Zahlen zu bilden.
- Das Passwort darf nicht identisch mit dem Benutzernamen sein.
- Die Gültigkeit ist beschränkt auf höchstens 365 Tage oder auf max. 5 Fehlversuche.

2.2.2. Nach max. 5 Fehlversuchen wird die Zugangsberechtigung gesperrt.

2.2.3. Fehlgeschlagene Zugriffsversuche (Sperren von Accounts) werden protokolliert.

3. Zugriffskontrolle (logisch)

Ziel: Verhinderung von unbefugten Zugriffen auf Daten des Leistungsbezügers durch berechtigte Systembenutzende.

3.1. Organisatorische Massnahmen:

3.1.1. Erarbeiten und Einrichten eines zweckmässigen und verbindlichen Berechtigungskonzepts auf der Basis definierter Benutzerrollen.

3.2. Technische Massnahmen:

3.2.1. Den Benutzern dürfen systemtechnisch nur die Rechte / Benutzerrollen zugewiesen werden, die im Berechtigungskonzept vorgesehen sind.

3.2.2. Mutationen bzw. Löschungen der Berechtigungen müssen unverzüglich nach Aufgabenwechsel oder dem Ausscheiden der Benutzer erfolgen.

3.2.3 Für externe Benutzer, welche privilegierten Zugriff auf Systeme des Kanton Solothurn benötigen, ist wenn möglich die Privileged Remote Access Lösung (PRA) des Kanton Solothurns zu verwenden.

4. Weitergabekontrolle

Ziel: Verhinderung des Verlustes der Vertraulichkeit, Verfügbarkeit und Integrität der Daten des Leistungsbezügers während der Übermittlung.

4.1. Organisatorische Massnahmen

4.1.1. Es sind Weisungen für die Verwendung von Datenübertragungsmitteln (Mail, Internet, Smartdevices usw.) zu erlassen.

4.1.2. Datenträger (Papier, Disketten, CDs, usw.) mit klassifizierten Daten müssen als solche bezeichnet und erkennbar sein.

4.1.3. Datenträger sind für den Versand geeignet zu verpacken und zu adressieren.

4.1.4. Es muss festgelegt und kontrolliert werden, welche Benutzer und Betreiber welche Netzwerkdienste beanspruchen dürfen.

4.2. Technische Massnahmen

4.2.1. Die Vertraulichkeit und Integrität von Authentifikationsdaten, Schlüsseln oder anderen kritischen Systemdaten muss bei der Übertragung der Daten über Netzwerke geschützt werden. Es sind Verschlüsselungsverfahren entsprechend dem Stand der Technik anzuwenden.

5. Eingabekontrolle

Ziel: Beweissicherung in Bezug auf die Benutzeraktivitäten.

5.1. Organisatorische Massnahmen:

5.1.1. Es muss verbindlich geregelt werden, wer welche Daten bearbeiten darf und wer die Verantwortung für den Datenschutz und die Datenqualität trägt.

5.2. Technische Massnahmen:

5.2.1. Entsprechende Logfiles für kritische System- und Datenänderungen sind automatisch durch das System zu erstellen und zu schützen.

6. Auftragskontrolle

Ziel: Gewährleistung der auftragskonformen Bearbeitung der Daten des Leistungsbezügers.

6.1. Organisatorische Massnahmen

(Im Rahmen dieser AGB unter 3.1 bereits geregelt)

6.2. Technische Massnahmen

6.2.1. Der Zugriff ist auf genau festgelegte Daten und Anwendungen zu beschränken.

6.2.2. Zugriffe über das Netz von aussen sind pro Anwendung mit vorgegebenen Authentisierungsverfahren (keine bis sehr starke 2-Weg Authentisierung) zu schützen.

7. Verfügbarkeitskontrolle

Ziel: Schutz der Daten des Leistungsbezügers vor eingeschränkter Verfügbarkeit, gegen Zerstörung und Verlust.

7.1. Organisatorische Massnahmen

7.1.1. Authentifikationsdaten des Systemverantwortlichen oder anderer privilegierter Systembetreiber müssen für notfallmässige Stellvertretungen in sicherer Form hinterlegt sein.

7.1.2. Für die Sicherheit von Betrieb, Nutzung und Wartung von Systemen und Anwendungen notwendige Dokumentationen müssen zu jeder Zeit bei den System- und Anwendungsverantwortlichen verfügbar sein.

7.2. Technische Massnahmen

7.2.1. Informatikräume und -systeme sind gegen physische Einflüsse (Einbruch, Brand, Wasser, usw.) angemessen zu schützen.

7.2.2. Systeme müssen durch einen Überspannungsschutz, eine unterbrechungsfreie Stromversorgung (USV) sowie durch eine entsprechende Klimatisierung geschützt sein.

7.2.3. Das Sichern von Daten auf Datenträgern (Backup) und das Zurückladen der Daten (Restore) muss regelmässig geprüft werden.

7.2.4. Mobile Datenträger müssen an geschützten und räumlich von der Betriebsumgebung abgegrenzten Orten aufbewahrt werden.

8. Organisatorische Massnahmen

(Im Rahmen dieser AGB bereits geregelt)

8.1. Technische Massnahmen

8.1.1. Test- und Produktionsdaten sind getrennt zu bearbeiten. Eine zuverlässige logische Trennung reicht aus.

9. Weitere Kontrollziele

Ziel: Generelle Gewährleistung der Informationssicherheit.

9.1. Organisatorische Massnahmen

9.1.1. Es sind angemessene Vorkehrungen für Stör-, Not- und Katastrophenfälle zu treffen.

(Weitere Bestimmungen im Rahmen dieser AGB nicht relevant)

9.2. Technische Massnahmen

9.2.1. Systeme und Anwendungen sind durch anerkannte Verfahren und Produkte gegen schadenstiftende Software (Malware etc.) zu schützen.

9.2.2. Ein sicheres Patchmanagement für Systeme / Software muss gewährleistet werden.

Anhang 2: Penetrationtests und Sicherheitsaudit

Systeme, welche Schnittstellen mit dem Internet und mindestens erhöhte Schutzanforderungen aufweisen, werden vor der produktiven Inbetriebnahme mittels einem Sicherheitsaudit überprüft. Sie müssen mindestens einen anhand des Schutzbedarfs definierten Risk Assessment Value (RAV) erreichen.

Penetrationstest vor Abnahme

Die Leistungserbringerin erklärt seine Bereitschaft, das von ihm entwickelte System vor der Abnahme einem Penetrationstest zu unterziehen. Der Test erfolgt durch einen vom Leistungsbezüger definierten Dienstleister und der Methode „Open Source Security Testing Methodology Manual" (OSSTMM; (de-facto Standard für Sicherheitsüberprüfungen)). Die Leistungserbringerin erklärt sich bereit, alle für den Test benötigten Ressourcen und Unterlagen zur Verfügung zu stellen. Der Penetrationstest ist Bestandteil der Abnahme eines Systems und wird durch den Leistungsbezüger organisiert, beauftragt und finanziert.

Für einen erfolgreichen Test gelten folgende Minimalziele:

- Penetrations-Test aller aus dem Internet erreichbaren Schnittstellen des Systems
- Risk Assessment Value (RAV) nach OSSTMM (zur Abnahmezeit aktuellste Version) des vereinbarten Wertes
- Es sind keine Verwundbarkeiten der Kategorie Vulnerability nach OSSTMM (zur Abnahmezeit aktuellste Version) vorhanden
- Erreichen des definierten Levels des OWASP Application Security Verification Standard (ASVS)

Falls obige Minimalziele nicht vollumfänglich erreicht werden, verpflichtet sich die Leistungserbringerin, alle nötigen Nachbesserung auf eigene Kosten durchzuführen und den Penetrationstest durch den externen Dienstleister zu seinen Lasten zu wiederholen.

Penetrationtests und Sicherheitsaudit nach der Inbetriebnahme

Die Leistungserbringerin erklärt ihre Bereitschaft, das von ihr entwickelte System nach vorgängiger Ankündigung durch den Leistungsbezüger weiteren Penetrationtests zu unterziehen. Diese werden vorgängig mit der Leistungserbringerin koordiniert und vom Leistungsbezüger organisiert, beauftragt und finanziert.
Die Leistungserbringerin erklärt sich bereit, Audits der relevanten Dokumente und Prozesse durch den Leistungsbezüger jederzeit durchführen zu lassen.