Ergänzende Vertragsbedingungen/Cyber Security Bedingungen
- Allgemein –
Stand: 17.09.2021

1. Allgemeine Bestimmungen

Die hier festgelegten Informationssicherheitsbestimmungen werden integraler Bestandteil des Hauptvertrages
Der Auftragnehmer muss die Informationssicherheitsanforderungen erfüllen und muss sicherstellen, dass sein Personal oder seine Subunternehmer diese ebenfalls erfüllen.
Die Einhaltung der Informationssicherheitsanforderungen muss zu jeder Zeit sichergestellt sein und regelmäßig seitens Lieferant auch für die Subunternehmer überwacht werden. (Auditrecht wird in Kapitel 11.4. geregelt)

2. Definitionen

Assets	Wie in ISO/IEC 27005 definiert, Assets umfassen primäre und unterstützende Vermögenswerte
Auftraggeber	Im Rahmen dieses Dokumentes ist hier primär der Betreiber Kritischer Infrastrukturen gemeint. Selbstverständlich kann in diese Rolle auch jeder andere Betreiber unterhalb des Sicherheitsniveaus „Kritische Infrastruktur“ einsteigen.
Auftragnehmer	Im Rahmen dieses Dokumentes ist der Hersteller und oder Lieferant gemeint, der als Vertragspartner des Auftraggebers auftritt.
Fernzugang	Zugang in das Netz des Auftraggebers – i. d. R. durch den Auftragnehmer
Kritikalität	Ein wichtiges Kriterium dafür ist die Kritikalität als relatives Maß für die Bedeutsamkeit einer Infrastruktur in Bezug auf die Konsequenzen, die eine Störung oder ein Funktionsausfall für die Versorgungssicherheit der Gesellschaft mit wichtigen Gütern und Dienstleistungen hat.
Penetrationstest	Ein Penetrationstest beschreibt die Prüfung der Sicherheit möglichst aller Systembestandteile und Anwendungen eines Netzwerks- oder Softwaresystems mit Mitteln und Methoden, die ein Angreifer anwenden würde, um unautorisiert in das System einzudringen (Penetration). Der Penetrationstest ermittelt somit die Empfindlichkeit des zu testenden Systems gegen derartige Angriffe.
Schwachstelle	Schwachstelle ist der in Organisationen (Unternehmen, Behörden) vorhandene organisatorische, prozessuale, personelle oder systemische Mangel, die die angestrebten Ziele beeinträchtigen und Schäden verursachen können.
Secure Code Review	Ein Secure Code Review ist eine spezielle Form des allgemeinen Code Reviews bei der mit Hilfe verschiedener Methoden noch bestehende Schwachstellen identifiziert werden.
Security by Design	Security by Design beschreibt die Integration von Sicherheitsaspekten in den vollständigen Lebenszyklus eines Produktes (Software, Hardware, Dienstleistung)

	bereits in der Design-phase des Produktes.
Service Level Agreement	Ein Service Level Agreement (SLA) ist Teil eines Servicevertrages. Zwischen Auftragnehmer und -geber werden verschiedenen Eigenschaften des Services, wie Umfang Qualität und Verantwortlichkeiten, vereinbart.
Security Level Agreement	Ein Security Level Agreement (SecLA) ist eine Sonderform der SLA mit dem Fokus auf Securityaspekten.
Schutzbedarfsanalyse	Im Rahmen der Schutzbedarfsanalyse werden sogenannte Schutzobjekte (schützenswerte Daten, Hardware, Infrastruktur etc. von Unternehmen) erkannt und mit einem realen Angriffsrisiko verknüpft.
Vulnerability Management	Prozess zur Erkennung und Behebung von Schwachstellen

3. Vulnerability-Management

Der Auftragnehmer unterzieht den Produkten einer kontinuierlichen Prüfung auf Schwachstellen, bspw. in Form eines sogenannten Vulnerability-Managements, um in der Lage zu sein, auf neue Schwachstellen so schnell wie möglich zu reagieren. Es basiert auf der Transparenz der Funktionalität, der technischen Architektur und von Unterkomponenten einschließlich der Betriebssysteme, Datenbanken, Server (z. B. Web, Telnet, SSH), Middleware und Bibliotheken. Diese wird verwendet, um neue Schwachstellen in Bezug auf die Kritikalität und die geschäftlichen Auswirkungen zu beurteilen.
Sind vom Auftragnehmer entwickelte Software-, Firmware- oder Hardware-Komponenten betroffen, ist der Auftragnehmer verpflichtet, umgehend die Schwachstellen an den Auftraggeber zu melden.

3.1. Methodik und Umfang

Jede Schwachstelle muss vom Auftragnehmer an den Auftraggeber gemeldet und bzgl. möglicher funktionaler und sicherheitsrelevanter Auswirkungen bewertet werden.

Der Umfang des Vulnerability-Managements umfasst jede potenzielle Schwachstelle, die möglicherweise Einfluss auf die Verfügbarkeit, Integrität und Vertraulichkeit der Vermögenswerte (materielle oder immaterielle) oder auf eine beim Auftraggeber operierende Dienstleistung des Auftragnehmers nehmen kann.

3.2. Vulnerability-Assessment

Der Auftragnehmer ist verpflichtet, kontinuierlich Quellen für Sicherheitsempfehlungen zu sichten und diese in Bezug auf die an den Auftraggeber gelieferten Assets zu bewerten. Sollte eine Komponente von der Sicherheitslücke betroffen sein, wird von dem Auftragnehmer erwartet, die Einstufung der Kritikalität und die zeitliche“ Bewertung durchzuführen (siehe Hinweise in Abschnitt 10).
Der Auftraggeber zeigt Verständnis dafür, dass die Informationen über die umliegende Infrastruktur oder andere einflussnehmende Umstände nicht vollständig sein können und dass das bestmögliche Ergebnis auf Basis des Wissens in dem Branchenumfeld des Auftragnehmers beruht.
Es sind mit dem Aufragnehmer Kriterien für Schwachstellen zu vereinbaren, bei denen der Auftraggeber vom Auftragnehmer oder Hersteller informiert werden muss und wie dieses erfolgen sollte.

3.3. Behebung von Schwachstellen

Die folgende Tabelle definiert die Kritikalität der Sicherheitslücken und die erwartete Zeit zur Implementierung einer Lösung:

- Finale Lösungszeit = Zeit benötigt für den Patch / die Wartungsfreigabe / die korrekte Installation der Lösung; Zeitraum, in dem auf den Service aus öffentlichen / externen Netzwerken zugegriffen werden kann.
- Zeit zur Neutralisierung = Zeit für eine vorläufige Lösung oder einen Workaround für den Fall, dass der Patch nicht innerhalb eines bestimmten Zeitrahmens verfügbar ist. Vom Auftragnehmer wird erwartet, dass eine Lösung mit einem Best-Effort-Ansatz und nach bestem Wissen erarbeitet wird. Die Zeitzählung beginnt mit der Benachrichtigung über die Schwachstelle.

Priorität	Kritikalitätsstufe	Finale Lösungszeit	Zeit zur Neutralisierung
1	hochkritisch	1 Monat	1 Tag
2	kritisch	3 Monate	3 Tage
3	weniger kritisch	6 Monate	14 Tage

Stellt eine Schwachstelle gleichzeitig eine Störung nach dem Hauptvertrag dar, so gelten für die Mängelbeseitigung die Reaktions- und Wiederherstellungszeiten des Hauptvertrages.

3.4. Kommunikation
Jegliche Kommunikationswege werden mit dem Auftragnehmer bzgl. Art und Form vereinbart. Kryptographische Techniken nach dem neuesten Stand der Technik müssen zur Geheimhaltung und Integrität für die Übermittlung dieser Mitteilungen verwendet werden.

4. Patch-Management
4.1. Patch-Umfang
Der Patch-Umfang muss das gesamte System, wie vom Auftraggeber akzeptiert, umfassen. Dazu gehören das Betriebssystem, alle Softwarepakete und Services des Betriebssystems, alle Tools und Applikationen des Herstellers zu Betriebs- und Wartungszwecken, die Zielapplikation (Servicelogik) und alle für den Service genutzten Middleware-Application-Layer, Datenbanken, Access-, Monitoring- oder Applikationsserver.

4.2. Patch-Level während der Systemabnahme
Der Auftragnehmer hat sicherzustellen, dass alle Systeme vor der Abnahme gepatcht und aktualisiert werden. Der Patch-Level sollte dabei nicht älter als sechs Monate ab dem Tag der Systemabnahmeerklärung sein. Der Auftragnehmer muss alle öffentlich verfügbaren und durch den Auftraggeber freigegebenen Patches als Teil der Lieferung installieren.

4.3. Patch-Management nach der Systemabnahme
4.3.1. Patch-Management-Lifecycle
Der Auftragnehmer verpflichtet sich, mindestens zweimal pro Jahr Updates und Patches bereitzustellen. Für die Bereitstellung durch den Auftragnehmer gelten die in Abschnitt 4.3 festgelegten Zeitrahmen.
Der Auftragnehmer verpflichtet sich für jede im Patchzyklus adressierte Schwachstelle einen detaillierten Bericht zu erstellen und dem Auftraggeber zur Verfügung stellen.

4.3.2. End of Life
Kündigt ein Drittanbieter eines Betriebssystems oder einer anderen Komponente (Software, Datenbanken, Anwendungen, etc.) das Ende des Lifecycles an, so kommuniziert der Auftragnehmer dies dem Auftraggeber so früh wie möglich, spätestens 6 Monate vor dem „End of Life“. Der Auftragnehmer aktualisiert entweder die Komponente auf die aktuellste neuere Version, setzt eine adäquate Alternative ein oder stellt einen erweiterten Support von Sicherheitspatches für die ältere Version vertraglich mit dem Drittanbieter sicher.

4.3.3. Lieferanten von reinen Anwendungen oder Funktionalitäten
In Fällen, in denen der Auftragnehmer nur Anwendungen und/oder andere Funktionalitäten liefert und der Auftraggeber oder sonstige Drittanbieter in seinem Namen für das Update-Management auf den darunterliegenden Schichten wie Betriebssystem verantwortlich ist, muss der Auftragnehmer eine kontinuierliche Funktionsfähigkeit seiner gelieferten Leistung auch bei Patches der darunterliegenden Systemplattform gewährleisten.

5. Systemhärtung
Der Auftragnehmer verpflichtet sich, die von ihm gelieferten Systeme zu härten, um die Auswirkungen potenzieller Sicherheitsrisiken zu minimieren. Dies muss vor der Deklaration einer Systemabnahme durch den Auftraggeber geschehen sein.

5.1. Minimale Installationsprinzipien
Es wird von dem Auftragnehmer erwartet, folgende Komponenten des Betriebssystems oder anderer Software zu installieren:
A. Jede Softwarekomponente, die für die Anwendung oder nach der Logik des Dienstes benötigt wird
B. Jede aus der Integration mit anderen Services resultierende andere Anwendung oder Softwarekomponente
C. Jede aus Betriebs- und Wartungsanforderungen resultierende Softwarekomponente
Jede andere Software darf nur in Abstimmung mit dem Auftraggeber installiert werden.

5.2. Netzwerkdienste (Netzwerkzugänge)
Jeder nicht benötigte Netzwerkzugang (TCP/IP- oder UDP-Port) muss deaktiviert sein. Die Nutzung jedes Zugangs muss in der Dokumentation des Auftragnehmers erläutert werden.

5.3. Konfigurationsstandards
Der Auftragnehmer stellt sicher, dass die vom Auftraggeber vorgegebenen allgemeinen Konfigurationsstandards und Sicherheitsvorschriften eingehalten werden.

5.4. Standardpasswörter
Der Auftragnehmer stellt sicher, dass jedes Standardpasswort in allen möglichen Fällen geändert werden kann.

5.5. Backdoors

Der Auftragnehmer muss im Rahmen seiner Möglichkeiten sicherstellen, dass seine Lösungen frei von „Backdoors“ sind, die die verwendeten Sicherheitsmechanismen umgehen können.

5.6. Kontrolle und Audit der in diesem Kapitel genannten Konditionen

Der Auftragnehmer verpflichtet sich, dass er hinsichtlich seiner Produkte mit geeigneten Maßnahmen und Protokollen, die mit dem Auftraggeber abzustimmen sind, nachweist, dass alle in diesem Kapitel genannten Anforderungen eingehalten werden.

6. Fernzugang für Drittanbieter

Fernzugänge von Drittanbietern zum Netzwerk des Auftraggebers und/oder dessen zugehörigen Unternehmen wird unter den folgenden Bedingungen gestattet. Prozess und Funktion dieses Zugriffs werden allein vom Auftraggeber definiert.

6.1. Allgemeine Erwartungen

Der Auftragnehmer muss sicherstellen, dass bei Fernzugängen die Vertraulichkeit, Verfügbarkeit und Integrität der Assets und Services des Auftraggebers gewährleistet sind. Dies beinhaltet auch die nachträgliche Verwendung von Informationen, von denen der Auftragnehmer während eines Fernzugriffes Kenntnis erlangt hat. Er ist für alle Aktionen der Benutzerkonten mit Fernzugangsfunktion auf Systemen des Auftraggebers verantwortlich.

6.2. User-Account-Management

Es wird allgemein erwartet, dass jeder Nutzer ein eigenes Nutzerkonto bereitgestellt bekommt. Der Auftraggeber zeigt Verständnis für Ausnahmen, sollten Umstände auftreten (Unternehmen mit mehreren Supportcentern und einer großen Anzahl an Personal), die dies erschweren.
Solche Ausnahmen müssen vorab dokumentiert und in einem SLA (Service Level Agreement) festgehalten werden. In diesem Fall wird der Auftragnehmer die komplette Rückverfolgbarkeit der Nutzung eines Accounts (wer, wann) festhalten (im besten Fall revisionssicher) und diese dem Auftraggeber auf Verlangen aushändigen.
Sollte die Situation auftreten, dass der Auftragnehmer ein Nutzerkonto nicht mehr benötigt, muss der Auftraggeber darüber unverzüglich informiert werden, so dass das entsprechende Konto gesperrt werden kann. Der Auftraggeber kann durch eine Betriebsfunktion oder eine alternative Service-Management-Funktion repräsentiert werden. Derartige Kontakte sind im SLA zu definieren.

Es wird vom Auftragnehmer erwartet, Nutzerkonten mit Fernzugangsfunktion alle sechs Monate zu überprüfen und den Auftraggeber über notwendige Änderungen zu informieren. Diesbezüglich sind Authentisierungsverfahren mit dem Auftraggeber zu vereinbaren.
Bei den physischen Einrichtungen sind die gesetzlichen Regelungen bezüglich Datenschutz und IT-Sicherheitsgesetz zu berücksichtigen.

7. Anforderungen an die Softwareentwicklungsprozesse

Die Berücksichtigung der Sicherheit in Entwicklungsprozessen (Security by Design) ist in vielen Fällen ein effizienterer Weg, um ein sicheres Softwareprodukt herzustellen, als das nachträgliche Patching und Ausrollen in der Produktion. Die Softwareentwicklungsprozesse des Auftragnehmers müssen so ausgelegt sein, dass der Sicherheit der entwickelten Software angemessene Beachtung in allen wichtigen Entwicklungsphasen geschenkt wird und die Prozesse sich an den allgemein anerkannten Industriestandards orientieren.
Insbesondere sollen folgende Punkte berücksichtigt werden:

- Vorhandene Standards der sicheren Softwarearchitektur
- Die Entwickler müssen sich an vorhandene Standards zur sicheren Programmierung halten, um Schwachstellen vorzubeugen. Diese Standards müssen dokumentiert werden und den Entwicklern z. B. in Schulungen bekannt gemacht werden.
- Secure-Code-Reviews als Teil der Qualitätssicherung und Testing. (Zum Beispiel müssen die eigenentwickelten Webapplikationen, die für den Betrieb in nicht geschützten Netzen vorgesehen sind, ein Code-Review nach einem Industriestandard wie OWASP durchlaufen.)
- Benutzung der Open-Source-Komponenten, angemessene Konfiguration, Dokumentation und Wartung dieser Komponenten
- Die Testverfahren beim Auftragnehmer sollen die implementierten Sicherheitsmechanismen und -funktionen (Verschlüsselung, Zugriffskontrollen, Authentisierung und andere) explizit beinhalten. Der Auftragnehmer stellt zu jeder Lieferung und zu jedem Update dem Auftraggeber die notwendige Menge von funktionalen Testfällen und -skripten zur Verfügung, die zum sicheren Funktionsnachweis benötigt werden.
- Sicherheitsüberprüfungen entsprechend den vorgesehenen Betriebsumgebungen, z. B. unabhängige Penetrationstests für die Systeme, die

aus den externen bzw. nicht abgesicherten Netzen erreichbar sein sollen.

- Ergebnisse der Secure-Code-Reviews bzw. Penetrationstests sollen dem Auftraggeber (zumindest für die finale Version des Produktes) zur Verfügung gestellt werden.

8. Einsatz der kryptographischen Lösungen

Um sicherzustellen, dass keine veralteten und als unsicher bekannten Kryptographielösungen in den Produkten verwendet werden, soll der Auftragnehmer eine schriftliche Richtlinie etablieren und mit dem Auftraggeber abstimmen, die die zulässigen Kryptographiealgorithmen definiert. Diese Richtlinie sollte sich an einen Industriestandard halten und regelmäßig überprüft werden.
Wenn eine Kryptographielösung in der Industrie als nicht mehr sicher bekannt wird, muss die Richtlinie angepasst werden. Wenn eine solche Kryptographielösung in dem bereits beim Auftraggeber eingesetzten Produkt verwendet wird, muss der Auftragnehmer sie im Rahmen vom Vulnerability-Management-Prozess (s. Abschnitt 3.) als Schwachstelle bewerten und melden**.** Der Lieferant hat Vorschläge zur Umgehung der Schwachstelle zu unterbreiten.
Der Auftragnehmer muss sicherstellen, dass der Einsatz der kryptographischen Absicherung der Kommunikation und Ablage überall erfolgt, wo es notwendig ist, um die Grundsätze der sicheren Softwarearchitektur zu unterstützen. Der Einsatz der kryptographischen Absicherung der Kommunikation ist insbesondere notwendig, wenn Daten mit hohem Schutzbedarf (z. B. Steuerungsdaten der Kritischen Infrastruktur oder vertrauliche Daten) über öffentliche oder als nicht ausreichend sicher geltende Netzwerke übertragen werden.

9. Dokumentation

Es wird vom Auftragnehmer erwartet, dass dieser jegliche Dokumentation zur Verfügung stellt, die die Nutzung der angebotenen Lösung erleichtert. Der gebräuchliche Umfang einer derartigen Dokumentation, wenn auch nicht auf diese beschränkt, inkludiert die folgenden Punkte:

- Liste der Hardware
- Liste der Software (inklusive Betriebssystem und Patch-Level)
- Überblick über die Systemarchitektur (kann Teil der Designdokumentation sein)
- Kommunikationsmatrix
- Existierende Benutzerkonten und Rollen sowie deren Berechtigungen
- Beschreibung von proprietären (nicht in der Industrie standardisierten) Sicherheitsmechanismen (Erwartung, die Prinzipien und Implementierung einer solchen Lösung zu verstehen)
- Weitere Dokumentationen, spezifiziert als Teil des Liefergegenstandes oder Auftrages, die die Sicherheit der Lösung gewährleisten

Sollten Änderungen an der gelieferten Lösung durchgeführt werden, wird vom Auftragnehmer erwartet, diese in die Dokumentation einzupflegen.

10. Benachrichtigung über sicherheitsrelevante Vorfälle

- Der Auftragnehmer ist verpflichtet, Sicherheitsvorfälle in seiner Organisation, die potenziell einen negativen Effekt auf materielle und immaterielle gelieferte oder auf dem Informationssystem gespeicherte Vermögenswerte haben könnten, umgehend ohne Zeitverzug dem Auftraggeber zu melden. Dies könnten z. B. auch Industriespionage oder eine Sicherheitslücke im Source-Code sein.
- Der Auftragnehmer wird im Falle eines Vorfalls auf Nachfrage des Auftraggebers Ressourcen zur Minderung und/oder Beseitigung des Vorfalles sowie den finalen Korrekturbericht bereitstellen.

11. Nicht-technische Sicherheit

11.1. Organisation der Informationssicherheit

Der Auftragnehmer hat dem Antrag des Auftraggebers nachzukommen, Informationen seiner Sicherheitsorganisation offenzulegen, auf dessen Basis der Auftraggeber eine Auftragnehmerbewertung durchführen kann. Diese Einschätzung ist ein interner Prozess, der den Auftraggeber dabei unterstützt, die Metriken und Reife der Sicherheitsorganisation des Auftragnehmers zu beurteilen.
Der Auftragnehmer soll, falls vorhanden, ein ISO27001-Zertifikat oder Äquivalente (Historie und Umfang) bereitstellen, sowie weitere Dokumente wie Berichte und Vorschriften etc. in diesem Kontext.

11.2. Asset-Management

Der Auftragnehmer hat alle Assets in seinem Informationssystem zu identifizieren und zu dokumentieren, die einen Bezug zum Informationssystem des Auftraggebers zwecks Wartung oder Betriebszugang haben können. Die Verantwortung für die Aufrechterhaltung der entsprechenden Sicherheitskontrollen dieser Assets muss zugewiesen werden. Die Assets sind zu dokumentieren. Diese Dokumentation ist

möglicherweise Teil des Audits (Abschnitt 11.4.), demnach werden alle Unterlagen vom Auftragnehmer schriftlich gepflegt.
Zum Schutz der Assets kann der Auftragnehmer die Anwendung spezifischer Sicherheitsmaßnahmen delegieren, jedoch bleibt der Auftragnehmer für den angemessenen Schutz der Assets, die in Bezug zu dem Informationssystem des Auftraggebers stehen, verantwortlich.
Die beim Auftragnehmer gespeicherten Daten müssen in dessen Besitz verbleiben (besonders Kundeninformationen), da er für die Daten haftet, z. B. im Falle von Datenverlust.

11.3. Human-Resources-Security

Jeder, der im Namen des Auftragnehmers agiert, der entfernten oder lokalen Zugriff auf das Informationssystem des Auftraggebers haben muss, muss Informationen zu seiner Identität bereitstellen. Der Auftragnehmer stellt sicher, dass in seinem Namen kein Zugang missbraucht wird und er die volle Verantwortung übernimmt, sollte sich herausstellen, dass dieser Fall eintritt.
Sollte der Auftragnehmer mit Subunternehmern zusammenarbeiten, um den Vertrag mit dem Auftraggeber zu erfüllen, muss der Auftragnehmer diesen ausdrücklich als Subunternehmer identifizieren und er muss sicherstellen, dass der Subunternehmer die gleichen Anforderungen erfüllt.
Auf Verlangen des Auftraggebers ist der Auftragnehmer verpflichtet, nur überprüftes Sicherheitspersonal, z. B. geprüft von nationalen Behörden, zum Umgang mit sensiblem Equipment einzusetzen, sowohl vor der der Integration in das Netzwerk des Auftraggebers als auch für die Wartung des sensiblen Equipments während der gesamten Betriebsphase. Relevante Informationen (insbesondere die Identifizierung und Bestimmung des sensiblen Equipments) müssen schriftlich vereinbart werden. Die von den lokalen gesetzlichen Bestimmungen festgelegten Ausnahmen sind zu beachten (so müssen z. B. für Auftraggeber in anderen Regionen, wie Afrika, Asien, Nordamerika sonstige Anforderungen entsprechend der örtlichen Gesetze geachtet werden).
Der Auftragnehmer beauftragt nur Personen, die über entsprechende Kenntnisse und Fähigkeiten bzgl. Installation, Soft- oder Hardware, Wartung oder Betrieb der Lösung verfügen.

11.4. Auditrecht

Der Auftragnehmer stimmt zu, dass der Auftraggeber oder ein anderer beauftragter Dritter im Auftrag des Auftraggebers die Organisation in Bezug auf die Informationssicherheit des Auftragnehmers auditieren darf. Dies kann einmal oder mehrmals geschehen. Die Prüfungen werden auf der Grundlage der von dem Auftragnehmer zur Verfügung gestellten Dokumentation durchgeführt. Der genaue Umfang, die Dauer und die Organisation werden jeweils einvernehmlich vereinbart.
Zusätzlich muss der Auftragnehmer die Abweichungen von den vereinbarten Sicherheits-anforderungen melden.