Vereinbarung zur Informationssicherheit

zwischen

N-ERGIE IT GmbH,

Am Plärrer 43

90429 Nürnberg

(nachfolgend Auftraggeber genannt)

und

<Firma>

<Straße>

<PLZ> <Ort>

(nachfolgend Auftragnehmer genannt)

Inhalt

Der Auftraggeber betreibt ein Informationssicherheitsmanagementsystem (ISMS) mit dem Ziel die Vertraulichkeit, Verfügbarkeit und Integrität der verarbeiteten Daten bzw. der relevanten Systeme sicherzustellen.

Auch Lieferanten leisten mit ihren Dienstleistungen und Produkten einen wichtigen Beitrag zur Informationssicherheit, weshalb mit dieser Vereinbarung entsprechende Regelungen definiert werden.

1 Dokumentation

Der Auftragnehmer stellt dem Auftraggeber eine Dokumentation der bereitgestellten Dienste und Systeme zur Verfügung.

Die Dokumentation soll insbesondere die folgenden Punkte umfassen:

- 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) Sicherheits-mechanismen
- Weitere Dokumentationen, spezifiziert als Teil des Liefergegenstandes oder Auftrages, die die Sicherheit der Lösung gewährleiten

Sollten Änderungen an der bereitgestellten Lösung durchgeführt werden, wird vom Auftragnehmer erwartet, diese in die Dokumentation einzupflegen und eine aktualisierte Fassung an den Auftraggeber zu übermitteln.

2 Asset-Management

Der Auftragnehmer erfasst und dokumentiert alle relevanten Hard- und Softwarekomponenten. Bei Software sollen die Softwareversion und das jeweilige Patchlevel angegeben werden. Die erfassten Daten sollen Bestandteil der in Abschnitt 0 beschriebenen Dokumentation sein.

3 Vulnerability-Management

Der Auftragnehmer muss seine Produkte einer kontinuierlichen Prüfung auf Schwachstellen unterziehen, bspw. in Form eines Schwachstellenscans oder einer Konfigurationsüberprüfung. Die letzte Prüfung darf zu keinem Zeitpunkt länger als 12 Monate zurück liegen, um in der Lage zu sein, auf neue Schwachstellen so schnell wie möglich zu reagieren. Das Vulnerability-Management berücksichtigt alle Komponenten der technischen Architektur einschließlich der Betriebssysteme, Datenbanken, Server (z.B. Web, SSH), Middleware und Bibliotheken. Die Ergebnisse werden verwendet, um neue Schwachstellen in Bezug auf die Kritikalität und die geschäftlichen Auswirkungen zu beurteilen.

Sind vom Auftragnehmer bereitgestellte 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. Zusätzlich sollen Schwachstellen auf technischer Ebene zum Beispiel nach CVSS2/CVSS3 oder einem Vergleichbaren System bewertet werden. Der Umfang des Vulnerability-Managements umfasst jede Schwachstelle, die möglicherweise Einfluss auf die Verfügbarkeit, Integrität oder Vertraulichkeit der Vermögenswerte (materielle oder immaterielle) oder auf eine beim Auftraggeber operierende Dienstleistung des Auftragnehmers nehmen kann.

Bei Bewertung der Kritikalität nach CVSS2/CVSS3, sollte eine Einstufung der Schwachstellen in die Stufen „kritisch“, „hoch“, „mittel“ und „niedrig“ - angelehnt an die Einstufung des „National Institute of Standards and Technology“[1] - erfolgen:

CVSS2-Score	CVSS3-Score	Kritikalitätsstufe
10	9.0-10.0	kritisch
7.0-9.9	7.0-8.9	hoch
4.0-6.9	4.0-6.9	mittel
0.0-3.9	0.0-3.9	niedrig

3.2 Vulnerability-Assessment

Der Auftragnehmer ist verpflichtet, kontinuierlich Quellen für Sicherheitsempfehlungen zu sichten und diese in Bezug auf die dem Auftraggeber zur Verfügung gestellten Assets zu bewerten. Sollte eine Komponente von der Sicherheitslücke betroffenen sein, wird von dem Auftragnehmer erwartet, die Einstufung der Kritikalität nach CVSS2/CVSS3 und die „zeitliche“ Bewertung durchzuführen.

Es können mit dem Aufragnehmer weitere Kriterien für Schwachstellen vereinbart werden, bei denen der Auftraggeber vom Auftragnehmer oder Hersteller informiert werden muss und wie dieses erfolgen sollte.

3.3 Behebung von Schwachstellen

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 des Auftragnehmers über die Schwachstelle.

Priorität	Kritikalitätsstufe	Finale Lösungszeit	Zeit zur Neutralisierung
1	kritisch	1 Monat	3 Tage
2	hoch	3 Monate	7 Tage
3	mittel	9 Monate	1 Monat
4	niedrig	Nach Absprache	Nach Absprache

[1] https://nvd.nist.gov/cvss.cfm

3.4 Kommunikation

Der Auftraggeber muss über identifizierte Schwachstellen ab der Kritikalitätsstufe „mittel“ unmittelbar informiert werden. Bei Schwachstellen niedriger Kritikalität genügt eine Sammelmeldung nach 30 Tagen.

Zur Meldung der Schwachstellen an den Auftraggeber müssen kryptographische Verfahren nach dem Stand der Technik zur Geheimhaltung und Integrität der Übermittlung dieser Mitteilung genutzt werden.

4 Patch-Management

Der Auftragnehmer muss alle eingesetzten Komponenten regelmäßig mit notwendigen Sicherheitsupdates versorgen, um etwaige Schwachstellen schnell zu schließen. Darüber hinaus müssen Bugs und Fehler innerhalb der Komponenten des Auftragnehmers durch Updates behoben werden.

4.1 Umfang des Patchings

Der Umfang des Patchings muss jede Komponente des Systems, wie vom Auftraggeber akzeptiert, umfassen. Dazu gehören in der Regel:

- Betriebssystem
- Alle Softwarepakete und Services, die Teil des Betriebssystems sind
- Alle Tools und Applikationen, die der Hersteller zu Betriebs- und Wartungszwecken installiert hat
- Zielapplikation (Servicelogik)
- Alle Middleware-Application-Layer, Datenbanken, Access-, Monitoring- oder Applikationsserver, die für den Service genutzt werden
- Netzwerkkomponenten
- Sicherheitskomponenten
- Management-Umgebungen und Clients

4.2 Patch-Level während der Systemabnahme

Der Auftragnehmer hat sicherzustellen, dass alle Systeme vor der Abnahme gepatcht werden. Der Patch-Level darf dabei nicht älter als 3 Monate ab dem Tag der Systemabnahmeerklärung sein. Der Auftragnehmer muss alle öffentlich verfügbaren 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 einzuspielen. Für die Bereitstellung sicherheitsrelevanter Patches durch den Auftragnehmer gelten hiervon unabhängig die in Abschnitt 3.3 festgelegten Zeitrahmen.

4.3.2 Ende des Lifecycle

Sollte für ein eingesetztes Produkt eines Drittanbieters, z.B. ein Betriebssystems oder eine andere Komponente (Software, Datenbanken, Anwendungen, etc.), das Ende des Lifecycles verkündet werden, muss der Auftragnehmer entweder:

- die Komponente auf die aktualisierte neuere Version migrieren,
- eine adäquate Alternative einsetzen,
- oder den weiteren Support von Sicherheitspatches für die ältere Version vertraglich mit dem Drittanbieter sicherstellen.

4.3.3 Ausnahmen bei Konflikten

Sollte zwingend notwendige Funktionalität durch eine verfügbare Aktualisierung deaktiviert oder eingeschränkt werden, so ist das weitere Vorgehen mit dem Auftraggeber abzustimmen. Dasselbe gilt, falls eine bestimmte Version einer Software benötigt wird, um Herstellersupport für ein anderes eingesetztes Produkt zu erhalten. Die jeweiligen Auswirkungen auf die Funktionalität und Sicherheit sind durch den Auftragnehmer aufzuzeigen.

4.4 Dokumentation und Nachweis

Die Durchführung des Patchens ist im Voraus zu planen und zu dokumentieren. Der Auftraggeber muss sowohl über geplante, als auch durchgeführte Patches informiert werden.

5 Systemhärtung

Der Auftragnehmer verpflichtet sich, die von ihm für die Erbringung der Dienste verwendeten Systeme zu härten, um die Auswirkungen potentieller Sicherheitsrisiken zu minimieren. Dies muss vor der Deklaration einer Systemabnahme durch den Auftraggeber geschehen sein. Der Auftragnehmer sollte sich hierbei an gängigen Vorgaben, wie z.B. aus dem BSI Grundschutzkatalog oder dem CIS-CAT orientieren. Insbesondere sind die nachfolgend beschriebenen Abschnitte einzuhalten.

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 nicht installiert werden, außer der Auftragnehmer und der Auftraggeber einigen sich darüber. Software die nur im Zeitraum der Installation notwendig ist, oder deren Installation nicht zu verhindern ist, ist nach Abschluss dieser zu entfernen. Nicht benötigte Rollen, Dienste und Funktionen sollten deaktiviert werden.

5.2 Netzwerkdienste (Netzwerkzugänge)

Jeder nicht benötigte Netzwerkzugang (TCP/IP- oder UDP-Port) muss gefiltert werden. 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 und vor Abnahme auch tatsächlich geändert wurde.

5.5 Backdoors

Der Auftragnehmer muss im Rahmen seiner Möglichkeiten sicherstellen, dass seine bereitgestellten Systeme 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 Benachrichtigung über sicherheitsrelevante Vorfälle

Der Auftragnehmer ist verpflichtet, Sicherheitsvorfälle in seiner Organisation, die potentiell einen negativen Effekt auf materielle und immaterielle gelieferte oder auf dem Informationssystem gespeicherte Vermögenswerte haben können, umgehend ohne Zeitverzug dem Auftraggeber zu melden. Dies könnte 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.

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:

- Etablierte Standards der sicheren Softwarearchitektur
- Die Entwickler müssen sich an etablierte Standards (z.B. OWASP Top 10, BIZEC, etc.) 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.
- Dokumentation und Aktualisierung von verwendeten Fremd-Komponenten (z.B: Open-Source Bibliotheken)
- Die Testverfahren beim Auftragnehmer sollen die implementierten Sicherheitsmechanismen und -funktionen (Verschlüsselung, Zugriffskontrollen, Authentisierung und andere) explizit beinhalten.

- Sicherheitsüberprüfungen entsprechend den vorgesehenen Betriebsumgebungen, z.B. unabhängige Penetrationstests für die Systeme, die aus den externen bzw. nicht abgesicherten Netzen erreichbar sein sollen.
- Ergebnisse relevanter Sicherheitsüberprüfungen müssen dem Auftraggeber zur Verfügung gestellt werden.

8 Sicherheitsanforderungen für den IT-Betrieb

8.1 Zugriffsschutz und Berechtigungsvergabe

Richtlinien, Prozesse und Kontrollen zum Zugriffsschutz und zur Berechtigungsvergabe müssen implementiert werden:

- Dokumentierte Freigabeprozesse für Berechtigungen auf Systemen und Informationen
- Prozesse zur zeitnahen Löschung von Zugriffsrechten bei Austritt oder Abteilungswechsel
- Nachvollziehbarkeit der Zugriffe
- Mehrfaktorauthentifizierung für sensible Systeme
- Richtlinien zum sicheren Umgang mit IT-Systemen, insbesondere:
    - Definierte und angemessene Passwortkomplexität und –gültigkeit
    - Bildschirmsperre nach Inaktivität

8.2 Einsatz der kryptographischen Lösungen

Um sicherzustellen, dass keine veralteten und als unsicher bekannten Kryptographielösungen eingesetzt werden, muss die Auswahl kryptographischer Mechanismen gemäß der jeweils aktuellen Fassung der BSI-Richtlinie TR-02102[2] erfolgen.

Wenn eine Kryptographielösung in der Industrie als nicht mehr sicher bekannt wird und eine solche Kryptographielösung in dem bereits beim Auftraggeber bereitgestellten Dienst bzw. der bereitgestellten Anwendung verwendet wird, muss der Auftragnehmer sie im Rahmen vom Vulnerability-Management-Prozess als Schwachstelle bewerten und melden. Der Auftragnehmer hat Vorschläge zur Behebung der Schwachstelle zu unterbreiten und nach Rücksprache umzusetzen.

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. Authentifizierungsdaten, personenbezogene Daten, Steuerungsdaten aus Prozess-Netzen oder vertrauliche Daten) über öffentliche oder als nicht ausreichend sicher geltende Netzwerke übertragen werden.

Die Klassifizierung der Daten ist Aufgabe des Auftraggebers und wird dem Auftragnehmer bei Auftragserteilung zur Verfügung gestellt.

[2] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

8.3 Security-Incident-Management

Der Auftragnehmer muss im Rahmen seiner Möglichkeiten Lösungen etablieren, um sicherheitsrelevante Ereignisse erkennen zu können. Dies umfasst beispielsweise die Auswertung sicherheitsrelevanter Ereignisse und die Verwendung dem Stand der Technik entsprechenden Erkennungsmechanismen. Prozesse zur Reaktion auf Sicherheitsvorfälle, sowie die dazugehörigen Rollen und Verantwortlichkeiten müssen definiert sein. Zur Meldung der Sicherheitsvorfälle s. den Abschnitt „Benachrichtigung über sicherheitsrelevante Vorfälle“.

8.4 Sicherheit in Auslagerungsprozessen

Wenn der Auftragnehmer Teile der Betriebsleistung oder anderer Dienstleistungen für den Auftraggeber an weitere Dienstleister auslagert, müssen die vom Auftraggeber in diesem Dokument beschriebenen Sicherheitsanforderungen in den Vereinbarungen mit den Dienstleistern berücksichtigt werden. Die Sicherheitsanforderungen mit den Dienstleistern müssen so definiert werden, dass die Sicherheitsstandards für die Daten des Auftraggebers und Leistungen für den Auftraggeber in jedem Fall eingehalten werden und dass der Auftragnehmer in der Lage ist, eigene Verpflichtungen zur Sicherheit gegenüber dem Auftraggeber vollumfassend zu erfüllen. Eine transparente Darstellung der durchgehenden Lieferkette einschließlich Subunternehmer ist gegenüber dem Auftraggeber nachzuweisen. Der Auftragnehmer muss den Auftraggeber im Vorfeld von Entscheidungen über die Auslagerung von Betriebs- oder Dienstleistungen informieren.

9 Nicht-technische Sicherheit

9.1 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 sicherheitsrelevanten Vorgaben des Auftraggebers umsetzt.

Der Auftragnehmer beauftragt nur Personen, die über entsprechende Kenntnisse und Fähigkeiten bzgl. Installation, Soft- oder Hardware, Wartung oder Betrieb der Lösung verfügen.

9.2 Externe Systemzugriffe

Einfügen falls relevant

Die vom Auftraggeber zur Verfügung gestellten externen Systemzugriffe müssen vom Auftragnehmer protokolliert werden. Hierfür muss wenigstens festgehalten werden:

- wer (Name des Mitarbeiters)

- wann und wie lange
- über welchen Zugang
- zu welchem Zweck
- auf welches System

9.3 Audits

Der Auftragnehmer stimmt zu, dass der Auftraggeber oder ein anderer beauftragter Dritter im Auftrag des Auftraggebers die relevanten Teile der Organisation, sowie die zum Produkt gehörenden Systeme in Bezug auf die Informationssicherheit des Auftragnehmers auditieren darf. Diese Überprüfung wird einmalig vor dem Go-Live der Software durchgeführt. 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 Abweichungen von den vereinbarten Sicherheitsanforderungen melden.

10 Ansprechpartner Informationssicherheit

Der Auftraggeber benennt einen Ansprechpartner, der in Angelegenheiten der Informationssicherheit vom Auftragnehmer kontaktiert werden kann. An ihn müssen auch sämtliche sicherheitsrelevanten Vorfälle gemeldet werden.

Der Auftragnehmer benennt ebenfalls einen qualifizierten Ansprechpartner für Informationssicherheit.

	Name	Funktion	Kontaktdaten
Auftrag-geber			
Auftrag-nehmer			

Folgenden Abschnitt einfügen, wenn relevant; Klärung und ggfs. Spezifizierung notwendig:

11 Regelungen bei Verstößen gegen diese Vereinbarung

Bei Verstoß gegen die Vereinbarungen dieses Vertrages wird eine Vertragsstrafe von XXX Euro vereinbart.

Anlage 1: Zentrale Anweisung C 3.21 – Richtlinie Sicherheit in der Informationstechnik

<Ort>, …….. Nürnberg, ……

Ort, den Ort, den

…… ……

(Auftragnehmer) (Auftraggeber)