RWE

Präqualifizierung Informationssicherheit IT / OT

RWE Aktiengesellschaft
RWE Platz 1
45141 Essen
Germany
www.rwe.com

Präqualifizierung Informationssicherheit IT / OT

1 Einleitung

Die **P**räqualifizierung **I**nformationssicherheit IT (Information Technology) / **O**T (Operational Technology) (**PIO**) ist im Rahmen des Verfahrens zur Gewährleistung eines angemessenen Schutzniveaus in der IT und OT (in der Büro-IT und Anlagentechnik) von Auftragnehmern auszufüllen. RWE stellt sicher, dass Dienstleister und Lieferanten ein Mindestmaß an Informationssicherheit zum Schutz der Organisation bei der Erbringung von Dienstleistungen erfüllen. Der Fragebogen gliedert sich in folgende Abschnitte:

Abschnitt 2: Allgemeine Angaben zum Unternehmen
Abschnitt 3: Liefer- und Leistungsumfang
Abschnitt 4: Bestätigung des Auftragnehmers

RWE ist dazu verpflichtet, innerbetriebliche und regulatorische Anforderungen zur Sicherheit der

- IT-Infrastruktur,
- Anlagentechnik,
- (intern oder extern) genutzten Datenverarbeitungssysteme sowie
- Informationswerte

umzusetzen, um die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten.

Als Betreiber kritischer Infrastrukturen (KRITIS / SEWD) ist RWE zusätzlich verpflichtet, bestimmte Anforderungen der Informationssicherheit auch innerhalb der Lieferkette sowie der Dienstleistungsverhältnisse sicherzustellen.

Dieser Fragebogen dient daher als Selbstauskunft für alle Lieferanten und Dienstleister des RWE Konzerns zur Einschätzung des aktuellen Informationssicherheitsniveaus Ihrer Organisation. Bitte beantworten Sie die PIO möglichst detailliert, vollständig und ausschließlich wahrheitsgemäß.

2 Allgemeine Angaben

Angaben zum Unternehmen	
Name:	
Telefon:	
E-Mail:	
Anschrift:	

Es ist ein zentraler Ansprechpartner zu benennen, der verbindliche Auskünfte zur Informationssicherheit – sowohl im internen Bereich als auch im Außenverhältnis zum Auftraggeber – geben kann. Für den Fall der Abwesenheit ist eine Vertretung vorzusehen.

Kontaktdaten des zentralen Ansprechpartners Informationssicherheit	
Name:	
Telefon:	
E-Mail:	
Optional: Kontaktdaten des Vertreters	
Name:	
Telefon:	
E-Mail:	

3 Liefer- und Leistungsumfang

Dieser Fragebogen umfasst zwei wesentliche Bereiche der Informationssicherheit:

- 3.1 Basisfragen **[verpflichtend für alle Auftragnehmer]**
- 3.2 Zusatzfragen OT **[verpflichtend für OT-relevante Auftragnehmer]**

welche abhängig von der angebotenen Dienstleistung des Auftragnehmers ausgefüllt werden müssen.

Damit diese Selbstauskunft der Informationssicherheit angemessen beantwortet werden kann, kreuzen Sie in der folgenden Tabelle alle relevanten Liefer- und Leistungsumfänge an und füllen Sie anschließend – je nach Liefer- und Leistungsumfang – die genannten Abschnitte aus.

Der Auftragnehmer erbringt Dienstleistungen in folgenden Bereichen:		
Auswahl	**Liefer- und Leistungsumfang**	**Abschnitte zur Bearbeitung**
☐	Beratung / Projektmanagement	**3.1**
☐	Brandmelde-, Feuerlösch- / Gefahrenmeldeanlagen	**3.1 & 3.2**
☐	Cloud (IaaS / PaaS / SaaS)	**3.1**
☐	Hardware Verkauf / Vermietung	**3.1**
☐	IT Installation & Wartung	**3.1**
☐	IT Outsourcing	**3.1**
☐	Leit- / Automatisierungs- / Fernwirktechnik	**3.1 & 3.2**
☐	Mess-, Steuerungs- & Regelungstechnik (vernetzt)	**3.1 & 3.2**
☐	Prozessdatenverarbeitung / Prozessdatennetz / Expertensysteme	**3.1 & 3.2**
☐	Schaltanlagen Leit- / Sekundär- / Schutztechnik (vernetzt)	**3.1 & 3.2**
☐	Software Lizenzen / Vermietung	**3.1**
☐	Softwareentwicklung	**3.1**
☐	Sonstiges (bitte beschreiben):	**3.1 / 3.2**

3.1 Basisfragen

Zertifizierungen und unabhängige Nachweise

3.1.1 Ist Ihre Organisation für den Liefer- und Leistungsumfang nachweislich von einem unabhängigen Dritten für den Betrieb eines Informationssicherheitsmanagement-systems (ISMS) zertifiziert? ☐ Ja ☐ Nein

☐ ISO/IEC 27001 Datum des Zertifikats:

☐ IT-Grundschutz Datum des Zertifikats:

☐ Sonstige (z.B. TISAX, CSA STAR) Datum des Zertifikats:

Beschreibung:

Wenn ja: deckt der Geltungsbereich der Zertifizierung den zu erbringenden Liefer- und Leistungsumfang ab? ☐ Ja ☐ Nein

Bitte fügen Sie die angegebene(n) Zertifizierung(en) / Nachweis(e) bei, inkl. Geltungsbereich (Scope) und Erklärung zur Anwendbarkeit (SoA)

! Sollten Sie eine gängige und gültige Zertifizierung / unabhängigen Nachweis beigelegt haben, sind die folgenden Fragen 3.1.2 bis 3.1.8 obsolet und müssen nicht beantwortet bzw. angekreuzt werden.

Regelungen zur Informationssicherheit

3.1.2 Ist ein Mitglied der Geschäftsleitung Ihres Unternehmens für die Entwicklung, Pflege und Herausgabe einer Informations- und Cybersicherheitsrichtlinie verantwortlich? ☐ Ja ☐ Nein

3.1.3 Verfügt Ihr Unternehmen über eine dokumentierte Richtlinie zur Informationssicherheit? ☐ Ja ☐ Nein

3.1.4 Wählen Sie die Sicherheitsbereiche aus, die in Ihren Richtlinien und Vorgaben zur Informationssicherheit behandelt werden:

a)	Zulässige Nutzung	☐ Ja	☐ Nein
b)	Datenschutz	☐ Ja	☐ Nein
c)	Fernzugriff /Kabellose Verbindungen	☐ Ja	☐ Nein
d)	Zugriffskontrolle	☐ Ja	☐ Nein
e)	Reaktion auf Informationssicherheitsvorfälle	☐ Ja	☐ Nein
f)	Verschlüsselungsstandards	☐ Ja	☐ Nein
g)	Daten- / Systemklassifizierung	☐ Ja	☐ Nein
h)	Antivirus	☐ Ja	☐ Nein
i)	Anschlussfähigkeit von Drittanbietergeräten	☐ Ja	☐ Nein
j)	Email / Instant Messaging	☐ Ja	☐ Nein
k)	Physische Sicherheit	☐ Ja	☐ Nein
l)	Personalsicherheit	☐ Ja	☐ Nein
m)	Netzwerk- / Perimetersicherheit	☐ Ja	☐ Nein
n)	Clean Desk	☐ Ja	☐ Nein
o)	Lieferanten / Dienstleister / Subunternehmer	☐ Ja	☐ Nein

3.1.5 Werden die Sicherheitsrichtlinien in regelmäßigen Abständen überprüft und auf den neuesten Stand gebracht? ☐ Ja ☐ Nein

3.1.6 Sind alle Sicherheitsrichtlinien für alle Nutzer einfach zugänglich (z.B. stehen im Intranet des Unternehmens)? ☐ Ja ☐ Nein

3.1.7 Führt Ihr Unternehmen Schulungen zum Thema Informationssicherheit für alle betroffenen Mitarbeiter durch? ☐ Ja ☐ Nein

3.1.8 Zusätzliche Dokumente als Nachweis (falls vorhanden): ☐ Ja ☐ Nein
Bitte als Anlage beifügen.

3.2 Zusatzfragen OT

Folgende Fragen sind verpflichtend auszufüllen, sofern der Auftragnehmer für den Auftraggeber Dienstleistungen im Bereich der Operational Technology (OT) erbringt.

Dies betrifft Dienstleistungen in folgenden Bereichen:

- Leit-, Automatisierungs- und Fernwirktechnik,
- Prozessdatenverarbeitung / Prozessdatennetz / Expertensysteme
- Anlagentechnik,
- Mess-, Steuerungs- und Regelungstechnik (vernetzt)
- Schaltanlagen Leit- / Sekundär- / Schutztechnik (vernetzt)
- Brandmeldeanlagen, Feuerlöschanlangen, Gefahrenmeldeanlagen.

Allgemeine Sicherheitsanforderungen Informationssicherheit OT			
3.2.1	**Zutritts-, Zugangs- und Zugriffsschutz**		
a)	Stellt Ihre Organisation sicher, dass alle Systeme, von denen unmittelbar oder mittelbar ein Zugriff auf Ressourcen aus dem OT-Bereich des Auftraggebers möglich ist, mit einem Zutritts-, Zugangs- und Zugriffsschutz versehen sind?	☐ Ja	☐ Nein
b)	Stellt Ihre Organisation durch geeignete organisatorische und technische Maßnahmen sicher, dass nur die berechtigen Mitarbeiter des Auftragnehmers Zutritt, Zugang und Zugriff zu den Ressourcen des Auftraggebers erhalten?	☐ Ja	☐ Nein
3.2.2	**Einsatz sicherer Passwörter**		
a)	Stellt Ihre Organisation für alle zur Zugangssicherung verwendeten Passwörter eine nach dem aktuellen Stand der Technik hohe Passwortgüte (z.B. gemäß der Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI)) sicher? **Bitte beschreiben Sie Anforderungen an Passwörter:**	☐ Ja	☐ Nein
b)	Liegt eine entsprechende Passwortrichtlinie vor?	☐ Ja	☐ Nein
c)	Wird die Passwortgüte durch technische Maßnahmen erzwungen bzw. sichergestellt?	☐ Ja	☐ Nein

d) Kommen zusätzlich zu Passwörtern weitere Sicherungsmaßnahmen (z.B. Multi-Faktor-Authentifizierung) zum Einsatz? ☐ Ja ☐ Nein

3.2.3 Verbot der privaten Nutzung

a) Stellt Ihre Organisation durch organisatorische oder technische Maßnahmen sicher, dass alle Systeme und Komponenten, von denen unmittelbar oder mittelbar ein Zugriff auf OT-Ressourcen des Auftraggebers möglich ist, nur für dienstliche Zwecke genutzt werden und dass eine private Nutzung durch die Mitarbeiter nicht zulässig ist? ☐ Ja ☐ Nein

b) Stellt Ihre Organisation durch technische oder organisatorische Maßnahmen sicher, dass private Komponenten der Mitarbeiter nicht für den Zugriff auf OT-Systeme des Auftraggebers benutzt werden dürfen bzw. dass sie nicht an Systeme bzw. Netze des Auftragnehmers angeschlossen werden dürfen, die für den Zugriff auf Ressourcen des Auftraggebers vorgesehen sind? ☐ Ja ☐ Nein

3.2.4) Wirksamkeit der Maßnahmen

Gibt es in Ihrer Organisation einen definierten Prozess, um alle technischen und organisatorischen Maßnahmen zur Informationssicherheit regelmäßig auf deren Wirksamkeit zu überprüfen (z.B. Audits, Assessments, PenTests)? ☐ Ja ☐ Nein

Bitte beschreiben Sie kurz den Prozess:

Die Ergebnisse sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

3.2.5) Sichere Entwicklung

Stellt Ihre Organisation durch organisatorische und /oder technische Maßnahmen sicher, dass bei der Entwicklung von Software, Hardwarekomponenten oder Systemen anerkannte Entwicklungs- und Qualitätsmanagementstandards eingehalten und unsichere Programmiertechniken und Funktionen vermieden werden? ☐ Ja ☐ Nein

3.2.6 Umgang mit Sicherheitsvorfällen und Sicherheitslücken

a) Gibt es in Ihre Organisation einen definierten Prozess, um Informationssicherheitsvorfälle (Incidents), welche den Auftraggeber, die Systeme des Auftraggebers oder die Erbringung des Liefer- und Leistungsumgangs direkt oder indirekt betreffen, unverzüglich an den Auftraggeber zu melden? ☐ Ja ☐ Nein

Bitte beschreiben Sie kurz den Prozess:

b) Stellt Ihre Organisation sicher, dass Sicherheitslücken oder Schwachstellen in Software, Hardwarekomponenten und Systemen, welche von Ihrer Organisation entwickelt oder als Bestandteil des Liefer- und Leistungsumfangs bereitgestellt werden, dem Auftraggeber unverzüglich bekannt gemacht werden? ☐ Ja ☐ Nein

Bitte beschreiben Sie kurz den Prozess:

c) Stellt Ihre Organisation sicher, dass Sicherheitslücken oder Schwachstellen, welche über interne oder externe Kanäle gemeldet oder bekannt werden, in einem angemessen Zeitrahmen behandelt und kommuniziert werden? ☐ Ja ☐ Nein
Die Kommunikation sollte auch dann unverzüglich erfolgen, wenn noch kein Patch zur Verfügung steht.

Bitte beschreiben Sie kurz den Prozess:

Verpflichtung von Mitarbeitern und Subunternehmern des Auftragnehmers

3.2.7 Sicherheitsunterweisung

a) Stellt Ihre Organisation sicher, dass alle Mitarbeiter über die sicherheitstechnischen Anforderungen der Ressourcen des Auftraggebers informiert sind?
Das betrifft insbesondere die möglichen Risiken, adäquate Gegenmaßnahmen sowie die persönlichen Verantwortungen der Mitarbeiter im Rahmen ihrer Tätigkeiten.
☐ Ja ☐ Nein

b) Sensibilisiert Ihre Organisation ihre Mitarbeiter zusätzlich in Bezug auf Informationssicherheit regelmäßig durch entsprechende Schulungen oder Mitteilungen?
Hierzu gehören auch sicherheitsbezogene Informationen bei Einführung neuer Techniken und Verfahren.
☐ Ja ☐ Nein

3.2.8) Datenschutz und Vertraulichkeit

Hat Ihre Organisation ihre Mitarbeiter auf die Einhaltung der datenschutzrechtlichen Bestimmungen, sowie auf die Vertraulichkeit der ihnen zugänglichen Daten (auch über das Ende ihrer Tätigkeit hinaus) verpflichtet?
☐ Ja ☐ Nein

3.2.9 Unteraufträge und Subunternehmer

a) Beschäftigt Ihre Organisation Unterauftragnehmer, die für die Erbringung der Lieferungen und Leistungen bei dem Auftraggeber notwendig sind bzw. eingesetzt werden?
☐ Ja ☐ Nein

b) Wenn ja, sind diese auf die Einhaltung der Informationssicherheitsrichtlinie(n) verpflichtet und wurde dies durch den Auftragnehmer dokumentiert?
Dies gilt auch für Arbeitnehmerüberlassungskräfte die beim Auftragnehmer eingesetzt werden.
☐ Ja ☐ Nein

Grundsicherung der Systeme

3.2.10 Systemhärtung und sichere Grundkonfiguration

a) Stellt Ihre Organisation sicher, dass alle Systeme und Netzwerkkomponenten, auf welchen Daten des Auftraggebers verarbeitet oder gespeichert werden, nach aktuellem Stand der Technik (z.B. gemäß der Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI)) gehärtet sind?
Dies bedeutet, dass unnötige Benutzerkonten, Applikationen, Netzwerkprotokolle, Dienste und Services zu deinstallieren, oder – falls eine Deinstallation nicht möglich ist – dauerhaft zu deaktivieren und gegen versehentliches Reaktivieren zu schützen sind.
Beschreibung der Maßnahmen:

☐ Ja ☐ Nein

b) Stellt Ihre Organisation durch geeignete Maßnahmen sicher, dass die sichere Grundkonfiguration dieser Systeme regelmäßig überprüft und dokumentiert wird?

☐ Ja ☐ Nein

3.2.11 Sicherheitsupdates

a) Stellt Ihre Organisation sicher, dass alle Systeme und Netzwerkkomponenten, auf welchen Daten des Auftraggebers verarbeitet oder gespeichert werden oder mit denen auf Systeme des Auftraggebers zugegriffen wird, mit aktuellen Software- / Firmwareversionen, Service-Packs und Sicherheits-Patches versehen sind?
Beschreibung der Maßnahmen:

☐ Ja ☐ Nein

b) Stellt Ihre Organisation durch geeignete technische oder organisatorische Maßnahmen sicher, dass der Patchstatus dieser Systeme regelmäßig überprüft und dokumentiert wird?

☐ Ja ☐ Nein

c) Stellt Ihre Organisation durch geeignete technische oder organisatorische Maßnahmen sicher, dass Sicherheitsupdates für das Betriebssystem und für Kommunikationsprogramme, mit denen auf Internetdienste zugegriffen wird, auf allen Systemen umgehend eingespielt werden? ☐ Ja ☐ Nein

3.2.12 **Antiviren- / Malwareschutz**

a) Stellt Ihre Organisation sicher, dass alle Systeme, auf welchen Daten des Auftraggebers verarbeitet oder gespei-chert werden oder mit denen auf OT-Systeme des Auftrag-gebers zugegriffen wird, über einen ständigen Virenschutz (On-Access-Scanner) und (tages-)aktuelle Viren-Pattern verfügen? ☐ Ja ☐ Nein

b) Stellt Ihre Organisation sicher, dass neben dem Virenschutz auf Arbeitsplatzsystemen gleichermaßen Viren-Scanner im Gateway- bzw. Serverbereich, bei Storagesystemen, sowie bei Systemen für den E-Mail-Versand, dem Webverkehr und dem Filetransfer eingesetzt werden? ☐ Ja ☐ Nein

Netzwerksicherheit

3.2.13 **Fernzugang / Remoteeinwahl**

a) Nutzt Ihre Organisation einen Fernzugang / eine Remoteeinwahl, um auf OT-Systeme oder OT-Komponenten des Auftraggebers zuzugreifen? ☐ Ja ☐ Nein

Nur falls ja: Fragen b) bis e) beantworten.

b) Wird dieser Fernzugriff vom Auftraggeber zur Verfügung gestellt? ☐ Ja ☐ Nein

c) Stellt Ihre Organisation durch geeignete organisatorische und technische Maßnahmen sicher, dass nur explizit autorisierte Mitarbeiter auf den Fernzugang zugreifen können? ☐ Ja ☐ Nein

d) Stellt Ihre Organisation durch geeignete organisatorische und technische Maßnahmen sicher, dass die Zugriffsrechte zu den Fernwartungssystemen so restriktiv wie möglich gehandhabt werden? ☐ Ja ☐ Nein

e) Stellt Ihre Organisation sicher, dass, falls ein Mitarbeiter seinen Aufgabenbereich wechselt oder das Unternehmen des Auftragnehmers verlässt, ihm umgehend die Zugangs- und Zugriffsberechtigung für den Fernzugang entzogen wird? ☐ Ja ☐ Nein

3.2.14 Schutz des internen Netzes

a) Ist das interne Netz Ihrer Organisation gegenüber dem Internet am Netzübergang durch eine Firewall, welche mindestens *Stateful Packet Inspection*-Funktionalität aufweist, geschützt? ☐ Ja ☐ Nein

b) Ist diese Firewall mit einem maximal restriktiven Regelwerk versehen, welches nur explizit benötigte und freigegebene Dienste erlaubt? ☐ Ja ☐ Nein

c) Ist diese Firewall so konfiguriert, dass direkte Zugriffe aus dem Internet in das interne Netz Ihrer Organisation unterbunden sind? ☐ Ja ☐ Nein

3.2.15 Kabellose Netze

a) Nutzt Ihre Organisation zur Erbringung der Lieferung und Leistungen kabellose Netze? ☐ Ja ☐ Nein

b) Falls ja: ist sichergestellt, dass diese kabellosen Netze angemessen gesichert sind, insbesondere durch starke Authentisierung und Verschlüsselung auf aktuellem Stand der Technik? ☐ Ja ☐ Nein

Beschreibung der Maßnahmen:

Wartungssysteme

3.2.16 Wartungssysteme zur Vor-Ort-Wartung

a) Stellt Ihre Organisation sicher, dass auf Wartungs- und Administrationssystemen, insbesondere auf mobilen Geräten, die beim Auftraggeber vor Ort direkt an OT-Systeme angeschlossenen werden, eine Firewall-Software installiert und aktiviert ist, die unberechtigte Zugriffe von außen verhindert? ☐ Ja ☐ Nein

b) Ist sichergestellt, dass die Firewall vom Benutzer nicht deaktiviert werden kann? ☐ Ja ☐ Nein

c) Stellt Ihre Organisation alternativ sicher, dass diese Systeme nie direkt an unsichere Netze wie z.B. das Internet angeschlossen werden? ☐ Ja ☐ Nein

3.2.17) **Sichere Administrations- und Wartungstools**

Stellt Ihre Organisation sicher, dass die Tools, die zur Administration und Wartung der OT-Systeme des Auftraggebers eingesetzt werden, über eine personalisierte Anmeldung, kryptographischen Schutz der Passworte, optional eine starke Authentisierung und eine Rechteverwaltung mit Einschränkung des Zugriffs auf den erforderlichen Umfang verfügen? ☐ Ja ☐ Nein

3.2.18 **Überprüfung auf Schadsoftware**

a) Stellt Ihre Organisation sicher, dass mobile Wartungs- / Administrations- und Parametrier- / Programmiergeräte über einen ständigen Virenschutz (On-Access-Scanner) und (tages-) aktuelle Viren-Pattern verfügen? ☐ Ja ☐ Nein
Hinweis: Vor einem Zugang zum OT-Bereich des Auftraggebers ist dieser Virenschutz zu aktualisieren!
Der Auftragnehmer hat auf Anfrage des Auftraggebers die getroffenen Vorsorgemaßnahmen unverzüglich im Detail darzustellen.

b) Stimmt Ihre Organisation zu, dass der Auftraggeber die vorgenannten Geräte sowie Speichermedien und Datenträger des Auftragnehmers jederzeit einer Überprüfung auf Schadsoftware mit geeigneter Anti-Schadsoftware unterziehen darf? ☐ Ja ☐ Nein

3.2.19) **Verschlüsselung von Festplatten und Wechseldatenträgern**

Stellt Ihre Organisation sicher, dass bei allen Systemen und Wechseldatenträgern, welche zur Vor-Ort- und Fernwartung der OT-Systeme des Auftraggebers verwendet werden, eine Datenträgerverschlüsselung nach Stand der Technik (z.B. Bitlocker) aktiviert ist? ☐ Ja ☐ Nein

3.2.20) **Rückwirkungsfreiheit für den OT-Bereich**

Kann Ihre Organisation garantieren, dass während der gesamten Erbringung der Lieferungen und Leistungen von allen Systemen und Wechseldatenträgern, welche zur Vor-Ort- und Fernwartung der OT-Systeme des Auftraggebers verwendet werden keine Gefährdungen für den OT-Bereich des Auftraggebers ausgehen? ☐ Ja ☐ Nein

4 Bestätigung

Unterschrift des Auftragnehmers

Der Auftragnehmer versichert, dass alle oben gemachten Angaben vollständig, wahrheitsgemäß und korrekt sind.

Alle Abweichungen zu den hier getätigten Angaben sind dem Auftraggeber unmittelbar zu melden.

Name (in Druckbuchstaben)

Ort, Datum

Unterschrift / Digitale Signatur