Prequalification Information Security IT/OT

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

RWE

Prequalification Information Security IT/OT

1 Introduction

The **P**requalification **I**nformation Security IT (Information Technology) / **O**T (Operational Technology) (**PIO**) is to be completed by contractors as part of the process to ensure an appropriate level of protection in IT and OT (in office IT and plant technology). RWE needs to ensure that providers and suppliers meet a minimum level of information security to adequately protect the organisation when providing services. The questionnaire is divided into the following sections:

Section 2: General company information

Section 3: Scope of supply and services

Section 4: Confirmation of the Contractor

RWE is obliged to comply with internal and regulatory requirements for the security of the

- IT infrastructure,
- Plant control technology,
- Data processing systems used (internally or externally), and
- Information assets

to ensure the protection goals of confidentiality, integrity and availability are met.

As an operator of critical infrastructures, RWE is also obliged to ensure certain information security requirements within the supply chain and service relationships are fulfilled.

This questionnaire therefore serves as a self-disclosure for all suppliers and service providers of the RWE Group to assess the current information security level of your organisation. Please answer the PIO as detailed, complete and truthful as possible.

2 General information

Details of the company	
Name:	
Phone:	
E-mail:	
Address:	

A central contact person must be appointed who can provide binding information on information security - both internally and in external relation to the client. An alternative should be appointed in case of absence.

Contact details of the central contact person for information security	
Name:	
Phone:	
E-mail:	
Optional: Contact details of the alternative contact person	
Name:	
Phone:	
E-mail:	

3 Scope of supply and services

This questionnaire covers two main areas of information security:

- 3.1 Basic questions **[mandatory for all contractors]**
- 3.2 Additional questions OT **[obligatory for OT-relevant contractors]**

which must be completed depending on the service offered by the contractor.

In order for this information security self-disclosure to be answered appropriately, tick all relevant supply and services in the following table and then - depending on the scope of supply and services - complete the sections mentioned.

The contractor shall provide services in the following areas:		
Selection	**Scope of supply and services**	**Sections to be edited**
☐	Consulting / Project Management	**3.1**
☐	Fire alarm systems, fire extinguishing systems, hazard detection systems	**3.1 & 3.2**
☐	Cloud (IaaS/PaaS/SaaS)	**3.1**
☐	Hardware sale / Leasing	**3.1**
☐	IT Installation & Maintenance	**3.1**
☐	IT Outsourcing	**3.1**
☐	Control / automation / telecontrol technology	**3.1 & 3.2**
☐	Measurement, control & regulation technology (networked)	**3.1 & 3.2**
☐	Process data processing / process data network / expert systems	**3.1 & 3.2**
☐	Switchgear control / secondary / protection technology (networked)	**3.1 & 3.2**
☐	Software licences / Leasing	**3.1**
☐	Software development	**3.1**
☐	Other (please describe):	**3.1 / 3.2**

RWE

3.1 Basic questions

Certifications and independent evidence

3.1.1 Does your organization operate an Information Security Management System (ISMS), which is certified by an independent third party? ☐ Yes ☐ No

☐ ISO/IEC 27001 Date of the certificate:

☐ IT-Grundschutz Date of the certificate:

☐ Other (e.g. TISAX, CSA STAR) Date of the certificate:

Description:

If yes: does the scope of the certification cover the scope of supply and services to be provided? ☐ Yes ☐ No

Please attach the specified certification(s)/evidence(s), incl. scope and statement of applicability (SoA)

! If you have enclosed a common and valid certification / independent evidence, the following questions 3.1.2 to 3.1.8 are obsolete and do not need to be answered or ticked.

Information security regulations

3.1.2 Is a member of your organization's senior management responsible for developing, maintaining and issuing an information and cyber security policy? ☐ Yes ☐ No

3.1.3 Does your company have a documented information security policy? ☐ Yes ☐ No

3.1.4 Select the security areas which are addressed within your information security policies and guidelines:

a)	Acceptable use	☐ Yes	☐ No
b)	Data privacy	☐ Yes	☐ No
c)	Remote access / wireless	☐ Yes	☐ No
d)	Access control	☐ Yes	☐ No
e)	Information security incident response	☐ Yes	☐ No
f)	Encryption standards	☐ Yes	☐ No
g)	Data / system classification	☐ Yes	☐ No
h)	Anti-virus	☐ Yes	☐ No
i)	Third-party connectivity	☐ Yes	☐ No
j)	Email / Instant Messaging	☐ Yes	☐ No
k)	Physical security	☐ Yes	☐ No
l)	Personnel security	☐ Yes	☐ No
m)	Network / Perimeter Security	☐ Yes	☐ No
n)	Clean Desk	☐ Yes	☐ No
o)	Suppliers / service providers / subcontractors	☐ Yes	☐ No

3.1.5 Are the information security policies reviewed and updated frequently? ☐ Yes ☐ No

3.1.6 Are all information security policies and standards readily available to all users (e.g. posted on company intranet)? ☐ Yes ☐ No

3.1.7 Does your company conduct information security training for all relevant employees? ☐ Yes ☐ No

3.1.8 Additional documents as proof of evidence (if available): ☐ Yes ☐ No
Please enclose as an attachment.

RWE

3.2 Additional questions OT

The following questions must be completed if the contractor provides services for the Operational Technology (OT) of the client.

This concerns services in the following areas:

- Control, automation and telecontrol technology,
- Process data processing / process data network / expert systems
- Plant engineering,
- Measurement and control technology (networked)
- Switchgear control / secondary / protection technology (networked)
- Fire alarm systems, fire extinguishing systems, hazard detection systems.

General security requirements Information security OT

3.2.1 **Physical and digital access protection**

a) Does your organisation ensure that all systems, with direct or indirect access to resources in the client's OT area, are provided with physical and digital protection? ☐ Yes ☐ No

b) Does your organisation ensure through appropriate organisational and technical measures that only authorised employees of the contractor are granted physical and digital access to the client's resources? ☐ Yes ☐ No

3.2.2 **Use of secure passwords**

a) Does your organization ensure a high password quality for all passwords used for access protection according to the current state of the art (e.g. according to the recommendations of the Bundesamt für Sicherheit in der Informationstechnik (BSI))? ☐ Yes ☐ No
Please describe the criteria for passwords:

b) Is there an appropriate password policy in place? ☐ Yes ☐ No

c) Is the password quality enforced or enforced by technical measures? ☐ Yes ☐ No

d) Are other security measures (e.g. multi-factor authentication) used in addition to passwords? ☐ Yes ☐ No

3.2.3 Prohibition of private use

a) Does your organization ensure through organisational or technical measures that all systems and components, withdirect or indirect access to the client's OT resources , are only used for business purposes and that private use by employees is not permitted? ☐ Yes ☐ No

b) Does your organisation ensure through organisational or technical measures that employees' private systems or components may not be used to access the client's OT systems i.e. that they may not be connected to the client's systems or networks which provide access to the client's resources? ☐ Yes ☐ No

3.2.4 Effectiveness of the measures

Does your organization have a defined process to regularly check the effectiveness of all technical and organisational information security measures (e.g. audits, assessments, pen tests)? ☐ Yes ☐ No

Please briefly describe the process:

The results shall be made available to the client upon request.

3.2.5 Secure development

Does your organization ensure through organizational and/or technical measures that the development and engineering of software, hardware components or systems comply with recognised development and quality management standards and that unsecure programming techniques and functions are avoided? ☐ Yes ☐ No

3.2.6 **Dealing with security incidents and vulnerabilities**

a) Does your organisation have a defined process for the immediate reporting of information security incidents, which directly or indirectly affect the client, the client's systems or the delivery of the goods and services, to the client? ☐ Yes ☐ No

Please briefly describe the process:

b) Does your organization ensure that security vulnerabilities or weaknesses in software, hardware components and systems developed by your organization or provided as part of the scope of supply and services are immediately disclosed to the client? ☐ Yes ☐ No

Please briefly describe the process:

c) Does your organization ensure that security vulnerabilities or weaknesses reported or disclosed via internal or external sources are dealt with and communicated in an appropriate timeframe? ☐ Yes ☐ No

Communication should take place immediately even if a patch is not yet available.

Please briefly describe the process:

Engagement of employees and subcontractors of the Contractor

3.2.7 Security awareness training

a) Does your organisation ensure that all employees are aware of the safety and security requirements of the client's resources?
This should include possible risks, adequate countermeasures and the personal responsibilities of the employees related to their work activities. ☐ Yes ☐ No

b) Does your organisation also educate its employees with regard to information security on a regular basis through appropriate training or communications?
This also includes security related information when new techniques and procedures are introduced. ☐ Yes ☐ No

3.2.8 Data protection and confidentiality

Has your organisation committed its employees to comply with data protection regulations, as well as to maintain the confidentiality of the data to which they have access (even beyond the end of their employment)? ☐ Yes ☐ No

3.2.9 Subcontracting and subcontractors

a) Does your organisation employ subcontractors who are used for the provision of the deliveries and services by the client? ☐ Yes ☐ No

b) If yes, are they required to comply with the information security policy(ies) and has this been documented by the contractor?
This also applies to temporary workers who are employed by the contractor. ☐ Yes ☐ No

Basic protection of the systems

3.2.10 System hardening and secure basic configuration

a) Does your organisation ensure that all systems and network components on which the client's data is processed or stored are hardened according to the current state of the art (e.g. according to the NIST guidelines)?
This means that unnecessary user accounts, applications, network protocols and services must be uninstalled or - if uninstallation is not possible - permanently deactivated and protected against accidental reactivation.
Description of the measures:

☐ Yes ☐ No

b) Does your organisation take appropriate measures to ensure that the secure basic configuration of these systems is regularly checked and documented?

☐ Yes ☐ No

3.2.11 Security updates

a) Does your organisation ensure that all systems and network components on which the client's data is processed or stored, or with which the client's systems are accessed, are provided with current software / firmware versions, service packs and security patches?
Description of the measures:

☐ Yes ☐ No

b) Does your organisation ensure through appropriate technical or organizational measures that the patch status of these systems is regularly checked and documented?

☐ Yes ☐ No

c) Does your organization take appropriate technical or organizational measures to ensure that security updates for the operating system and for communication programmes used to access internet services are promptly applied to all systems?

☐ Yes ☐ No

3.2.12 Antivirus / malware protection

a)	Does your organisation ensure that all systems on which the client's data is processed or stored, or with which the client's OT systems are accessed, have constant virus protection (on-access scanner) and (daily) up-to-date virus patterns?	☐ Yes	☐ No
b)	Does your organisation ensure that, in addition to virus protection on workstation systems, virus scanners are also used in the gateway or server systems, in storage systems, as well as in systems for sending emails, web traffic and file transfer?	☐ Yes	☐ No

Network security

3.2.13 Remote access / remote dial-in

a)	Does your organization use remote access / dial-in to access OT systems or OT components of the client?	☐ Yes	☐ No
	Only if yes: answer questions b) to e).		
b)	Is this remote access provided by the client?	☐ Yes	☐ No
c)	Does your organization ensure through appropriate organisational and technical measures that only explicitly authorised employees can access remote access?	☐ Yes	☐ No
d)	Does your organisation take appropriate organisational and technical measures to ensure that access rights to remote maintenance systems are handled as restrictively as possible?	☐ Yes	☐ No
e)	Does your organization ensure that if an employee changes job responsibilities or leaves the contractor's organisation, his or her remote access and access privileges are immediately revoked?	☐ Yes	☐ No

3.2.14 Protection of the internal network

a)	Is your organisation's internal network protected from the Internet at the network gateway by a firewall that has at least stateful packet inspection functionality?	☐ Yes	☐ No
b)	Is this firewall equipped with a maximally restrictive set of rules that only allows explicitly required and approved services?	☐ Yes	☐ No
c)	Is this firewall configured to prevent direct access from the Internet to your organization's internal network?	☐ Yes	☐ No

3.2.15 **Wireless networks**

a) Does your organization use wireless networks to deliver supplies and services? ☐ Yes ☐ No

b) If yes: have you ensured that these wireless networks are adequately secured, in particular through strong authentication and state-of-the-art encryption? ☐ Yes ☐ No

Description of the measures:

Maintenance systems

3.2.16 **Maintenance systems for on-site maintenance**

a) Does your organisation ensure that a firewall software is installed and activated on maintenance and administration systems, especially on mobile devices that are directly connected to OT systems at the client's site, to prevent unauthorised access from outside? ☐ Yes ☐ No

b) Have you ensured that the firewall cannot be deactivated by the user? ☐ Yes ☐ No

c) Alternatively, does your organization ensure that these systems are never connected directly to insecure networks such as the internet? ☐ Yes ☐ No

3.2.17 **Secure administration and maintenance tools**

Does your organisation ensure that the tools used to administer and maintain the client's OT systems have personalised login, cryptographic protection of passwords and if required strong authentication and rights management limiting access to the required functionality? ☐ Yes ☐ No

3.2.18 **Check for malware**

a) Does your organization ensure that mobile maintenance / administration and parameterisation / programming devices have permanent virus protection (on-access scanner) and (daily) up-to-date virus patterns? ☐ Yes ☐ No
Note: Before accessing the OT area of the client, this virus protection must be updated!
Upon request of the client, the contractor shall immediately present the precautionary measures taken in detail.

b) Does your organization agree that the client may at any time subject the aforementioned devices as well as (hard-) disks and storage media of the contractor to a check for malware with suitable anti-malware software? ☐ Yes ☐ No

3.2.19 **Encryption of hard disks and removable media**

Does your organisation ensure that state-of-the-art disk encryption (e.g. Bitlocker) is activated on all systems and removable disks as well as media used for on-site and remote maintenance of the client's OT systems? ☐ Yes ☐ No

3.2.20 **Freedom of retroactivity for the client's OT systems**

Can your organisation guarantee that throughout the provision of the supplies and services, all systems and removable disks and media used for on-site and remote maintenance of the client's OT systems do not pose any risks to the client's OT systems? ☐ Yes ☐ No

4 Confirmation

Signature of the contractor

The Contractor warrants that all the information provided above is complete, true and correct.

Any deviations from the information given here must be reported immediately to the Client.

Name (in block capitals)

Place, date

Signature / Digital Signature