Prequalification Information Security OT

RWE Generation SE
RWE Platz 3
45141 Essen
Germany
www.rwe.com

RWE Power AG
RWE Platz 2
45141 Essen
Germany
www.rwe.com

RWE Generation NL
Amerweg 1
4931 NC Geertruidenberg
Netherlands

RWE Generation UK
Windmill Hill Business Park
Whitehill Way
SN5 6PB Swindon
United Kingdom

RWE

Prequalification Information Security OT

1 Introduction

As an Operator of Essential Services (OES), RWE is obliged to comply with legal and internal requirements for the information security of its

- OT infrastructure (Operational Technology),
- plant control technology,
- plant technology, and
- information assets

in order to ensure the protection needs of availability, integrity and confidentiality.

For this reason, RWE must also ensure certain information security requirements within the supply chain as well as service relationships that affect these plants, systems and components.

All suppliers and service providers shall meet a minimum level of information security within their own organization when providing services for these systems and infrastructures.

This Prequalification Information Security OT (PIO) is an element of the procedures that ensure an appropriate level of information security of OT infrastructures operated by RWE. It is to be completed by all contractors providing relevant services.

This questionnaire therefore serves as a self-disclosure for all suppliers and service providers of the RWE companies to assess the current level of information security of your organization and the systems of your organization that are required for the delivery of services.

This prequalification is **not** intended to evaluate the security level of the plants, systems and components to be supplied.

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

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**
☐	Control / automation / telecontrol technology
☐	Measurement, control & regulation technology (networked)
☐	Process data processing / process data network / expert systems
☐	Switchgear control / secondary / protection technology (networked)
☐	Fire alarm systems, fire extinguishing systems, hazard detection systems
☐	Software development
☐	Cloud (IaaS/PaaS/SaaS)
☐	Consulting / Project Management
☐	Penetration testing / simulated attacks in OT systems
☐	Other (please describe):

RWE

4 Certifications and Security Policies

Certifications and independent evidence

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

4.2 If yes: what certification(s)/evidence(s) of the following can be submitted? (Multiple selections possible)

☐ ISO/IEC 27001 Date of the certificate:

☐ IT-Grundschutz (German Federal Office for Information Security) Date of the certificate:

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

Description:

4.3 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 4.4 to 4.10 are obsolete and do not need to be answered or ticked.

Information security regulations

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

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

RWE

4.6	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

4.7	Are the information security policies reviewed and updated frequently?	☐ Yes	☐ No
4.8	Are all information security policies and standards readily available to all users (e.g. posted on company intranet)?	☐ Yes	☐ No
4.9	Does your company conduct information security training for all relevant employees?	☐ Yes	☐ No
4.10	Additional documents as proof of evidence (if available): **Please enclose as an attachment.**	☐ Yes	☐ No

5 Detail questions OT

General security requirements Information security OT			
	Physical and digital access protection		
5.1	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
5.2	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
	Use of secure passwords		
5.3	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 CIS Benchmark, German Federal Office for Information Security (BSI) or UK National Cyber Security Centre (NCSC))? **Please describe the criteria for passwords:**	☐ Yes	☐ No
5.4	Is there an appropriate password policy in place?	☐ Yes	☐ No
5.5	Is the password quality enforced or enforced by technical measures?	☐ Yes	☐ No
5.6	Are other security measures (e.g. multi-factor authentication) used in addition to passwords?	☐ Yes	☐ No
	Prohibition of private use		
5.7	Does your organization ensure through organisational or technical measures that all systems and components, with direct 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

5.8	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

Effectiveness of the measures

5.9	Does your organization have a defined process to regularly check the effectiveness of all organisational information security processes and measures (e.g. audits, assessments)? **Please briefly describe the process:**	☐ Yes	☐ No
5.10	Does your organisation have a defined process to regularly check the effectiveness of all technical processes and measures for information security (e.g. audits, pen tests, red teaming)? **Please briefly describe the process:**	☐ Yes	☐ No

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

Secure development

5.11	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
5.12	Does your organisation use automated procedures as part of the development process to check source code, libraries used and other programme components for vulnerabilities and unsafe programming techniques?	☐ Yes	☐ No

Dealing with security incidents and vulnerabilities

5.13 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:

5.14 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:

5.15 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

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

Please briefly describe the process:

5.16 Is your organisation required by law, regulation or contract to report security breaches, vulnerabilities or incidents? ☐ Yes ☐ No

Please list the organisations to which you report the above events:

Disposal and repair of systems

5.17 Does your organisation have a defined process to ensure that systems or components that are sent for repair or disposal no longer contain confidential or security-relevant data? Yes No

Security of systems in transit

5.18	Does your organisation ensure through a defined process that systems or components with confidential or security-relevant data or systems intended for use in OT facilities of the client are secured against unauthorised access along the entire transport route?	Yes	No

Compliance with legal requirements

5.19	Does your organisation ensure, through a defined process, that legal, regulatory or other information security requirements are met in the regions or countries where supplies or services are provided? **Please briefly describe the process:**	Yes	No

Business Continuity / Management of Emergencies

5.20	Does your organisation have defined business continuity processes to ensure that in the event of an emergency or major disruption, a minimum quality of service is maintained and that all services to be provided to the client are restored as quickly as possible?	Yes	No
5.21	Are these business continuity processes tested at regular intervals, e.g. as part of emergency or disaster recovery exercises? **Please briefly describe the process:**	Yes	No

Protection of confidential data

5.22	Does your organisation take organisational and/or technical measures to ensure that confidential or security-relevant data or information relating to the provision of goods and services to the client or the client's OT facilities and systems are stored securely and protected from unauthorised access?	Yes	No

Please briefly describe the process:

5.23	Is this data or information protected from unauthorised access even if it is stored outside the contractor's premises or networks (e.g. in cloud systems or on mobile devices or portable storage media)?	Yes	No

Remarks / exclusions (please give reasons):

RWE

Engagement of employees and subcontractors of the Contractor

Security check

5.24	Does your organisation have a defined process in place to ensure that newly hired employees, who have access to OT systems or client data, are subject to a security or background check before taking up employment **Please briefly describe the process:**	☐ Yes	☐ No
5.25	Does your organisation carry out regular (subsequent) security and background checks for all employees, who have access to OT systems or client data?	☐ Yes	☐ No

Security awareness training

5.26	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
5.27	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

Data protection and confidentiality

5.28	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

Subcontracting and subcontractors

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

Please list the subcontractors:

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

Remarks / exclusions (please give reasons):

Basic protection of the systems

System hardening and secure basic configuration

5.31	Does your organisation ensure that all your organisation's systems and network components on which the client's data is processed or stored or which are used to access the client's OT systems are hardened according to the current state of the art (e.g. according to the CIS Benchmarks or NIST guidelines)? This includes 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
5.32	Does your organisation take appropriate measures to ensure that the secure basic configuration of these systems is regularly checked and documented?	Yes	No

Security updates

5.33	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
5.34	Does your organisation ensure through appropriate technical or organizational measures that the patch status of these systems is regularly checked and documented?	☐ Yes	☐ No
5.35	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

Antivirus / malware protection

5.36	Does your organisation ensure that all systems of your organisation 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
5.37	Does your organisation ensure that, in addition to virus protection on your organisation's 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

Local administrator privileges

5.38	Do users have local administrator privileges on your organisation's individual workstation computers?	☐ Yes	☐ No
5.39	Do administrators have local administrator privileges on your organisation's individual workstation computers?	Yes	No
5.40	Do developers have local administrator privileges on your organisation's individual workstation computers?	Yes	No
5.41	Do (service) technicians have local administrator privileges on your organisation's individual workstation computers?	Yes	No

Vulnerability scans

5.42	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 are scanned for weaknesses or vulnerabilities at regular intervals and according to the current state of the art?	☐ Yes	☐ No

Remarks / exclusions (please give reasons):

Network security

Remote access / remote dial-in into networks of the supplier

5.43	Does your organisation provide its employees or (sub-)service providers with remote access or dial-in that allows them to directly or indirectly access OT systems or OT components of the client?	Yes	No

Remote access / remote dial-in into networks of the client

5.44	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 5.45 to 5.48.

5.45	Is this remote access operated and provided by the client?	☐ Yes	☐ No

If No, please provide details of the remote access:

5.46	Does your organization ensure through appropriate organisational and technical measures that only explicitly authorised employees can access remote access?	☐ Yes	☐ No

5.47	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
5.48	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

Protection of the internal network

5.49	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
5.50	Is this firewall equipped with a maximally restrictive set of rules that only allows explicitly required and approved services?	☐ Yes	☐ No
5.51	Is this firewall configured to prevent direct access from the Internet to your organization's internal network?	☐ Yes	☐ No
5.52	Does your organisation monitor internet gateways for (attempted) intrusions and anomalous or malicious activities?	☐ Yes	☐ No

Data transmission via public networks

5.53	Does your organisation take technical measures to ensure that unauthorised or unusual data transfers (e.g. unusually large amounts of data, unexpected types of network traffic or traffic to unknown destinations) between internal and public networks are detected and prevented? **Description of the measures:**	☐ Yes	☐ No

Wireless networks

5.54	Does your organization use wireless networks to deliver supplies and services?	Yes	No
5.55	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:

Remarks / exclusions (please give reasons):

Maintenance systems

Maintenance systems for on-site maintenance

5.56	Does your organisation ensure that a firewall software (e.g. OS integrated firewall) is installed and activated on your organisation's 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
5.57	Have you ensured that this firewall software cannot be deactivated by the user?	☐ Yes	☐ No
5.58	Alternatively, does your organization ensure that your organisation's maintenance and administration systems are never connected directly to insecure networks such as the internet?	☐ Yes	☐ No

Secure administration and maintenance tools

5.59	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

Check for malware

5.60	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? Note: Before accessing the OT area of the client, this virus protection must be updated!	Yes	No

Upon request of the client, the contractor shall immediately present the precautionary measures taken in detail.

5.61	Does your organization agree that the client may at any time subject the aforementioned devices as well as (hard-) disks and storage media provided or used by your organisation to a check for malware with suitable anti-malware software. This includes permitting the client to check systems for malware prior to use in the client's facilities.	Yes	No
5.62	Does your organisation agree that the client may check storage media and data drives of the contractor for malware with suitable anti-malware software (e.g. in a data scanning terminals) prior to use in the client's facilities?	Yes	No

Encryption of hard disks and removable media

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

Freedom of retroactivity for the client's OT systems

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

Remarks / exclusions (please give reasons):

6 Confirmation

Signature of the contractor

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

The Contractor assures to notify RWE immediately via the responsible purchasers of any subsequent deviations from the information provided here.

Name (in block capitals)

Place, date

Signature / Digital Signature