Information Technology Provisions of the Regional Booking Platform

The processes and requirements determining the appropriate level of information technology security of RBP are listed in the following chapters. The processes shown below ensure the availability and protection of RBP and its system elements as well as the confidentiality, integrity and availability of data handled on RBP in a way that is proportionate to the arising risks. The information technology security levels and the processes ensuring them are updated and defined according to the stipulations of the ISO 27001:2006 standard.

1 The scope and characteristics of information security

'confidentiality of data': only those authorised and only to the extent of their authorisation shall obtain access to, use and determine the use of the data

'integrity of data': the content and characteristics of the data correspond to the requirements, including the certainty that the data originate from the required source (authenticity) and the certainty of origin (undeniability)

'integrity of the system element': the system element can be used for the intended purpose

'availability of data and the elements of RBP': they can be used by those authorised at the required time and for the required duration

'command': RBP is an event-driven system, where every interaction in the system is described as a complex command, consisting of instructions and data

'command store': every command is stored in the core memory, constituting the command store

'continuity': protection exists despite the circumstances and conditions changing with time

'proportionality to risks': in an adequately long interval the costs of protection are proportionate to the potential damage value

2. Secure information processing applied in the operation of RBP

2.1 Validation checking of inbound data

Checking of inbound data is supported by automated, predefined, rule-based, limited validation processes from the aspect of both content and form. The correctness of the validated inbound data lies in the sole responsibility of the sender.

2.2 Integrity of inbound data – logging

For logging the user or operation activity, the application saves every input data in a database (when and what was modified, initialized by the user). A time stamp in UTC form is attached to every entry. User activity may be analysed from the logs.

3. System operation

Command-store (logs) supports both troubleshooting and analysis of system use.

RBP's internal service supports the handling of customer complaints and unpredictable operational situations using the log in a way that by re-running the stored commands (including inbound data) in the configuration, separated from the productive system. In that

environment the system can be built up, up to a certain moment of time, then can be shifted, thus the potential reported problems can be reconstructed and demonstrated.

3.1 Checking the internal processing

Sophisticated real time monitoring and alarming system further internal, scheduled consistency checks ensure the integrity of the system.

3.2 System-wide data consistency

RBP is an integrated, independent system, where communication between functional group of nodes and databases take place using high-speed, reliable technical solution called Oracle streaming.

3.3 Checking outbound data

The application ensures the accuracy and consistency of outbound data thanks to the use of standard technology.

3.4 Validation of outbound data

Where required, the authenticity of outbound documents is validated with an electronic signature.

4 Operational processes related to information security

4.1 Access to the operating RBP system

In the RBP productive and RBP test environments a certificate-based authentication is in use. RBP can only be accessed with an individual digital certificate, which is provided by an approved Certification Authority or Registration Authority and granted to identify the appropriate person.

The below rules shall apply when managing authorisation:

- Authorisation requests and refuses are kept on record,
- Authorisation is granted only after sufficient registration,
- Security checks/audits are regularly held on the information technology systems, network devices, applications etc. that are relevant to RBP.

4.1.1 Managing privileged authentications

In RBP's production or test or systems, a wide range of customisable, authorised permissions can be assigned to the application's users. Authorisation always requires an electronic key issued by a certification authority.

4.2 Managing services of a third party

When a third party is involved, the security measures, operation processes, service definitions and levels of service are laid down in the agreements concluded for providing the service. Services provided by the third party are continuously monitored and internally audited.

4.3 Protection and maintenance of devices

Protection measures are applied to the effect of environmental threats and dangers maintain at the lowest possible level. Attempts at unauthorised access to the system are monitored and suspicious events generate immediate alarm and direct reactions.

Maintenance of the devices is carried out according to the maintenance plan defined by the device manufacturer and internal rules, which ensures the professional maintenance of the infrastructure at the prescribed intervals of time.

4.4 IT resource management

In order to reduce the shortage of resources, utilisation is monitored using a redundant monitoring system and its records are analysed at regular intervals, as part of the proactive operational safety.

4.5 Backups

As a result of the regular risk assessments the backup processes prescribe the following:

- List of data-groups, configuration data, software to be saved,
- Secure storage of backup tapes,
- Saving and restoring processes, their acceptable parameters,
- Supervised long-term operational data store.

4.6 Managing network security

The following rules have been applied when establishing network security:

- Separate network segments are established,
- Firewall protection is provided towards the internet,
- Firewall rules are maintained according to strict operational codes,
- Virus protection solutions are installed and maintained (where relevant),
- Secure data transmission channels are used when connecting information technology systems (e.g. SSH, SFTP, SSL, TLS, etc.),
- In order to facilitate the retrieval of security incidents, a log is kept of the firewall dataflow,
- The configuration of active network devices is saved,
- The security parameters, service levels and process control requirements are regulated in appropriate internal codes and contracts.

5. Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

The RBP Operator provides the necessary measures, including but not limited to the infrastructure, the operation of the infrastructure and the required qualified personnel either directly or via subcontractors so that the continuous and required service level of operation is ensured. Redundancy of system elements has been established, on one hand within the used state-of-the-art servers, storage systems and network equipment and using parallel running (hot-parallel) server groups in local and remote backup sites on the other. Business and technological risks are continuously examined, analysed and the findings of the assessments are utilised in the operation of RBP, as well as in defining the Business Continuity Plan and the Disaster Recovery Plan.

5.1. BCP

The BCP can only be initiated if the restoration of normal operations of the RBP cannot be expected within a foreseeable and calculable timeframe, and it endangers the provision of normal business processes.

The BCP process can only be initiated by the RBP Operator. All affected TSO Members and Network User Members have to be notified in written form about the initiation of the BCP process by the RBP Operator without undue delay via email or fax.

Shall the services of the RBP be unavailable in spite of the redundant hardware and software architecture; the following measures have to be taken.

5.1.1. BCP for Yearly, Quarterly and Monthly Capacity Auctions

The RBP Operator offers a centralised YQM BCP service for its TSO Members.

The RBP Operator shall announce the commencement of the BCP procedure without undue delay.

In case of yearly, quarterly and monthly capacity auctions, the Parties shall agree on a new auction start date that should fall no later than 5 (five) business days from the originally planned start date of the given auction. The capacity auction shall be repeated on the agreed new auction start date.

5.1.2. BCP for Daily Auctions

The RBP Operator shall announce the commencement of the BCP procedure without undue delay.

The daily auction shall not be repeated. Instead, the first within-day auction for the given gas day shall be considered as the backup solution for the daily auction.

5.1.3. BCP for Within-Day Capacity Auctions

In case of any issues preventing or disabling the scheduled running of within-day capacity auctions, the RBP Operator shall inform the relevant TSO Member(s) and Network User Member(s) without undue delay about the unavailability of the relevant within-day capacity auctions.

The RBP Operator shall make all reasonable efforts to eliminate the cause of the error preventing the scheduled operations of the within-day auctions.

Due to the time limitations of the scheduling of within-day capacity auctions, within-day capacity auctions may not be repeatable. In such cases, the RBP Operator shall announce without undue delay the commencement of the scheduled within-day auctions once the relevant subsequent within-day capacity auctions become again available.

Upon the warning of the RBP Operator, the TSO Member may start its own within-day BCP procedure (if any).

5.2. DRP

Disaster recovery may be required in case of severe failures. System restoration and data restoration is ensured by rebuilding the previous state of the system and data from system and data backup. In case of hardware failures, parts of or the whole system of RBP has to be restored by external service provider. In case of data restoration, the external service provider as well as the RBP Operator can restore data. Real-time backup ensures that all recorded data preceding the disaster event may be restored.