Annex

INFORMATION SECURITY DESCRITPION

1 GENERAL

1.1 About this document

The Energy Market Authority and WM-Data Novo have agreed on the security issues of the Emissions Trading Registry according to WM-Data Novo's general principles that are presented in this document. Detailed security procedures are kept confidential to maximize overall security of the Emissions Trading Registry. More information can be obtained from:

Jukka Moisanen, Energy Market Authority
Lintulahdenkatu 10
FIN-00500 Helsinki
Finland
Tel. +358 9 6220 360

Juha Kuntonen, WM-Data Novo
Valimotie 15 B
FIN-00381 Helsinki
Finland
Tel. +358 40 833 0595

2 COMMON INFORMATION SECURITY ISSUES

2.1 Organisation and responsibilities in WM -data Novo

The President & CEO is in overall charge of data security, while the IT Board supplies the related directions, and Senior Vice Presidents are in charge of data security within their profit centres. While those in charge of data security within business units ensure its enhancement within their units' products and services, WM-data Novo's IT administration attends to its in-house development.

Every WM-data Novo employee, and those of its partners, must take data security into account in the firm's operations and services, throughout the latters' lifecycle.

IT -board is the steering group of Information Security. Company Information Manager is responsible of developing Information security, including security policies and guidance.

Information security is integrated in WM -data quality management and company security management.

2.2 Service Auditing

The customer may audit the service with agreed methods. Auditing is limited to delivered service. The auditing time, auditing method and audit plan will be agreed in good time.

3 SECURING CONTINUITY IN SERVICES

The IT service continuity is simplified by on four key elements: physical environment, IT, people and process. The disaster and recovery plan lays on managing daily operation.

Redundant network links, power sources, processing power, and storage facilities, are key elements in IT environment continuity. Building and Facility Access are secured by badges that must be worn and personal access rights to secured areas. Any change of employment status is automatically and quickly fed into the security system.

Video surveillance is located in data rooms, parking lots and peripheral areas. All critical IT systems have UPS protection. Fire suppression and prevention systems are located in critical areas. There are fire stopping walls or air spaces between your facility and others

There are internal operations manuals list steps and escalation policies to limit the impact of failures and problems. System operators are trained and knowledgeable regarding operating procedures and practices for maintaining availability of critical information systems.

System documentation is located in a system database. The database includes information of data system f.e. system criticality levels, system components, manuals etc. The database is kept up to date when changes in IT infrastructure are done.

There are several ways to insure the availability of IT systems and insure continuity. WM-data Novo has defined a base level of security incl. continuity. In critical systems customized and system specific disaster and recovery plan will be done cooperating with the customer.

4 SECURITY PRINCIPLES FOR THE DELIVERY OF SERVICES AT WM-DATA NOVO

4.1 Service Delivery

The management of security within a system is based on a careful security assessment carried out in co-operation with our customer, and its subsequent realisation. Upholding the security of our services is an elementary part of WM-data Novo's daily operations. A system delivery is performed in accordance with mutually agreed and controlled operating models.

4.2 Starting an Information System Project

We deliver an information system service to the customer as a project in accordance with the so-called Novo Model, our system and project work method which ensures the high quality and security of the service throughout its life cycle.

The delivery includes a risk analysis which we carry out at the starting phase in co-operation with our customer. After this, we agree on system-specific risk management methods and security arrangements.

For these data security preparations, we recommend that our customer appoints both the person responsible for the company's IT matters and the person familiar with the actual operations. The supplier will be represented by a person who is familiar with the system or software in question.

Should a need arise during the project to increase the security methods and upgrade the security level, related measures and costs will be agreed on separately.

4.3 Specification

The detailed requirements for the information system, its information and function content as well as structure are defined. Data material is classified on the basis of its confidentiality, and information systems on the basis of their importance for the customer. For each security category we define a data security level with specific data security measures and instructions.

4.4 Follow-up and Quality Control

The customer has the right to monitor the delivery of the service insofar as this is possible in view of safeguarding the operations of WM-data Novo, its other customers and interest groups.

Before a system is implemented, its security is verified. This auditing is carried out by evaluating whether the service has been realised in accordance with the pre-specified security level.

4.5 Information Flow Planning

Information flow planning includes the definition of the persons whom the service concerns, both in the customer and the supplier organisation. To ensure the flow of information, both parties nominate contact persons with clearly specified responsibilities.

4.6 Support Functions Planning

Support functions are defined in connection with implementation planning. Support functions planning includes the nomination of support persons and training them for the various areas of responsibility; agreeing on communication methods between the customer and WM-data Novo; and agreeing on practices aimed at the rapid settlement of possible errors or other failures.

Support functions planning consists the following:

- support functions charting; what kind of support is needed, in addition to training, to ensure the production use of the system or software

- information flow planning; how the communications related to the system or software will be handled, both between the users and between the customer and supplier

- agreeing about service practicalities; how to handle as smoothly as possible any errors, malfunctioning or development needs discovered in the system or software at the beginning of the production use.

4.7 Protecting the Data Processing Environment

The protection of data within systems is carried out mainly through user identification and access rights control. The information systems with specific requirements for confidentiality and non-repudiation normally contain an identification system based on strong identification. The identification level will be agreed upon separately with the customer if necessary.

With respect to data communications, the systems can be protected against intruders through an IDS system, a systematic configuration of firewalls and other data processing components, as well as throrough control and logs. The protection of data communications will be tailored for each customer.

4.8 Physical Environment

The criticality of the system and hardware impacts on physical security requirements. Hardware placement will be separately agreed upon with each customer. The physical circumstances of the hardware are measured, controlled and monitored around the clock.

With respect to the physical environment, protection against intruders is taken into account in addition to the security of the production environment. This will be carried out through personnel guidance and control as well as arrangements related to the physical premises, among other things. Also external workforce, such as subcontractors' service personnel, will be taken into account.

4.9 Rights of Use and Access Rights

Data security, taking into account the different types of storage media, is planned in such a manner that the data is protected against intentional or unintentional handling by outsiders.

In addition to the storage media, the control of the rights of use and access rights applies to the physical environment, servers, network components and data transfer channels, among other things. The control procedures related to the rights of use will be agreed upon separately if needed.

WM-data Novo personnel use separate user ids and a safe password policy to enable auditing and protect against password guessing attacks. It is possible to use stronger authentication if necessary. WM-data policy applies to all service layers specified.

In the case of Emissions Trade Register system, WM-data assumes responsibility of user rights administration and password policy for operating systems and database. The users, their privileges, method of authentication and password policy of the Emissions Trade Register application are determined by Energy Market Authority.

4.10 Software

Data security matters related to off-the-shelf software products have normally been defined, designed and realised at a general level when the software was constructed. If there is a need for it and the software enables it, data security features can be further tailored according to the customer's requirements in connection with the implementation stage. Customer-specific tailoring must be agreed upon in good time so that we will have time to realise and test everything.

4.11 Hardware

The security requirements for an individual device stem from the requirements for the system attached to it. These affect, for example, service agreements, configuration, architecture and hardware and software solutions. To make it easier to manage the system entity, we aim at a consistent whole which is also coherent and standardised and takes open interfaces into account, and has been found good in practice.

A hardware register supports hardware management. As a general rule, it is maintained in databases in which information on hardware criticality, software data, customers, the supplier, responsible persons, network interfaces and instructions are available to the service personnel.

4.12 System and procedures for safeguarding of data

Backing up and restoring data is dedicated to a backup team. There are currently four administrators responsible for operational tasks related to backups. Centralized servers are backed up under the Supplier's Service centralized backup system. The Supplier is responsible for backing up software licenses and equipment. Server backup is based on a rotational basis. Full backup is made once a week and modified data is backed up daily. Weekly backups are retained for one month and monthly backups for one year from the time of backup. Backup is made daily between 23.00 – 06.00. Backup is made with an automatic backup system, located in a different combustion chamber.

The aim of data backup is to ensure files are restored to their original after a failure of some kind. Data backups and restorations are performed according to the backup/restore plan, which was defined with the Customer. The Customer is responsible for ensuring that the Suppliers backup plan includes all targets, which are needed to correctly backup the system.

Backup media and physical sites: weekly backup media is stored at the STK9310 Tape Library (Valimotie 17, Helsinki) and monthly backup media is transferred to an archive room and stored in DataSafes, which have the highest possible fire classifigation: S 120 DIS EN 1047-1. Data Safes are located in Valimotie 15, Helsinki. Server backup is based on a rotational basis. Full backup is made once a week and modified data is backed up daily. Weekly backups are retained for one month and monthly backups for one year from the time of backup.

Legato Networker and Tivoli Storage Manger-backup software keeps track of the monitor performance of backup tasks including notification of

backup failures, log review, spot checks, audit, management reporting, identification of scope and content of backup procedures (i.e., database, application software, server logs, etc.).

4.13 Network

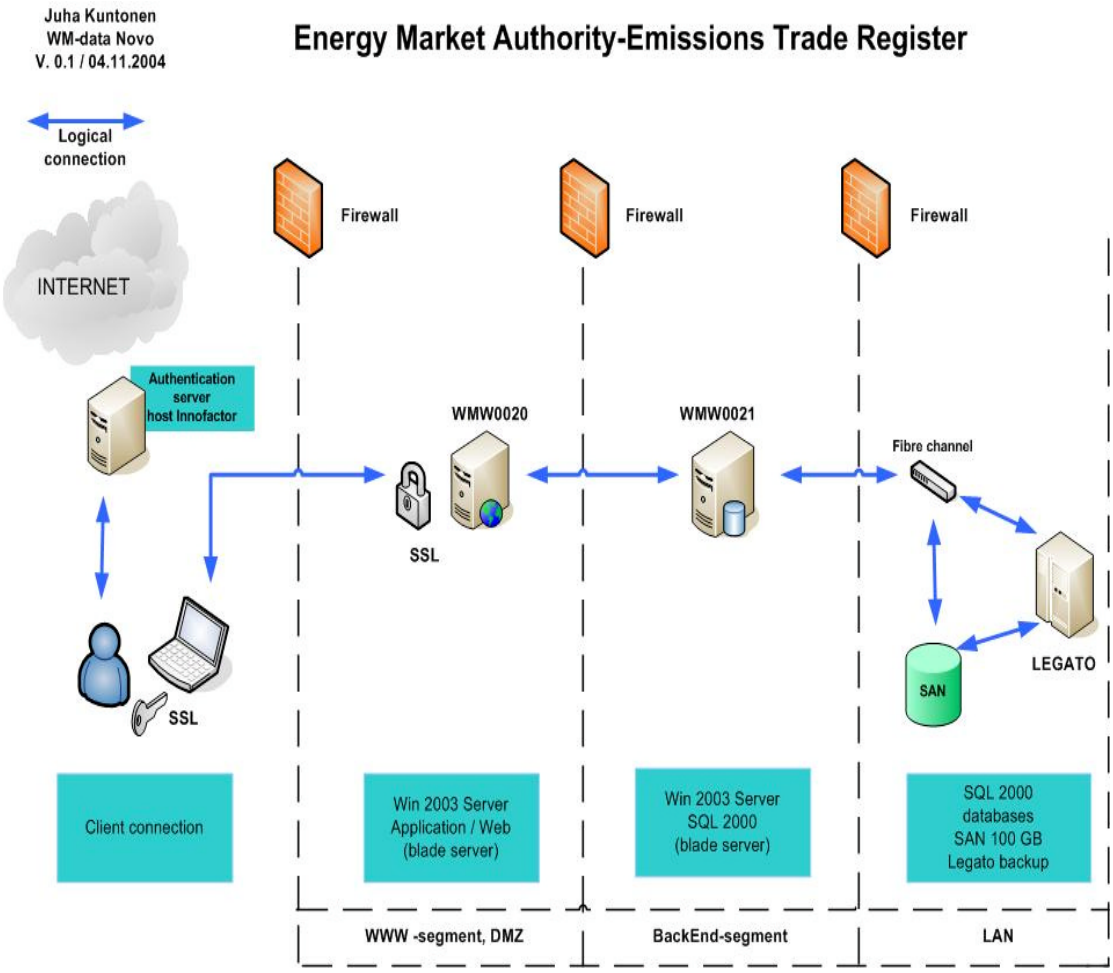
Network protection methods are always agreed upon separately with each customer. The use of the Internet, teleworking and networking require that the connections are protected, in particular against unauthorised use.

Communication over Internet is secured very professional manner by WM-data including following protocols and methods such as SSL-encryption, VPN-connections etc.

WM-data is utilized most recent technology in order to active the highest possible security level.

The security requirements for a system are taken into account in firewall system design. These requirements impact on the following, among others:

- acquisition of a firewall and related software
- documentation, training and system support
- installation
- implementation
- log-in and alarm systems



4.14 Realisation and implementation

In the realisation phase, the technical solutions and software are realised and tested, and the necessary operating manuals are drawn up. If the customer's data security solutions require customer-specific tailoring, it is carried out at this stage.

The data security solutions required by a new system or software (such as rights of use and protection) are realised and tested in the production environment. In this way we make sure that it works as required and that the system has no security gaps.

The customer-specific data security requirements related to a system have been taken into account early at the construction stage, in connection with specification, design and realisation. These can be further specified in the implementation phase, also with respect to the production environment.

The maintenance personnel and users are trained for their tasks and the safe use of the system. Designs and manuals are kept in a place where they are easily available to relevant persons. Document storage is organised in such a manner that the destruction of an individual place of storage or storage medium has been taken into account.

4.15 Service Maintenance

The successful maintenance of the service requires that the customer and Novo have a shared view about the service content and its security requirements.

Maintenance is organised in accordance with the agreement concluded with the customer. The system is monitored to ensure its functionality and capacity.

4.15.1 Control and Management

The purpose of the control of the hardware managed by Novo is to control the customer's network and the active hardware connected to the network, to identify any and interruptions in time and to initiate preventive measures, as well as to maintain and develop the control system. The control and management procedures are tailored for each customer.

4.15.2 Change Management

A change of the system version may be necessary if there are changes in the operating environment. Any changes will be agreed upon with the customer, except for such minor changes in the production environment which are not customer-specific and do not affect the general security level of the service.

4.16 Deinstallation/transfer

In the case of deinstallation, the system functions are run down in a controlled manner. We agree upon the handling of the system's information content with the customer. Documentation, programmes and data are filed insofar as necessary or handed over to the customer. Other data is destroyed in a manner agreed upon with the customer.

In the case of deinstallation, we design and realise the necessary system security changes in those systems which are connected to the system to be deinstalled.

We also carry out any changes necessary in the rights of use as a result of the system deinstallation. These changes and procedures will be documented and handed over to the customer for approval.

5 DIVISION OF RESPONSIBILITY MATRIX - EMISSIONS TRADE REGISTER

Responsibility by task and system component

Task	system component	Energy Market Authority	WM-data Novo	Innofactor Oy	notes
monitoring	*physical & network*	I	R		includes security incidents
create alerts	*operating system (W2003)*	I	R		log auditing and security
resolve incidents	*database (SQL 2000)*	I	R		incident investigation are
restore service level	*application (emission trade)*	I		R	not included in basic monthly fee
access control	*physical & network*		R		
user administration	*operating system (W2003)*		R		
grant & revoke permission	*database (SQL 2000)*		R		
	application (emission trade)			R	
monitor security updates	*physical & network*	I	R	I	
submit change request for	*operating system (W2003)*	I	R	I	
security patches	*database (SQL 2000)*	I	R	I	
install patches	*application (emission trade)*	I	I	R	
data back up and restore			R	A	

Responsibility by ITIL service support process

Process	Subprocess				vendor's role
Incident management		R	A	A	assists in resolving incidents
Problem management		R	A	A	provide data for problem mgmt
Change management	Evaluate & analyse change	R	A	A	provide work & cost estimates
	Authorise change	R	I	I	
	Testing	R		A	
	Implement change	R	A	A	actual implementation *
	Post-implementation review	R	I	I	
Release management		A	A	R	
Configuration management		R	A	A	document system components
Security management	define security policy	R	A	A	

Notes

"*Physical & network*" includes
server equipment, data communications, datacenter facilities and shared equipment
* = not included in basic monthly fee

Responsibility codes are:

R	is responsible for the task/process
A	assists in the task/process
I	is informed of the task/process and its outcome