IT requirements for suppliers

Below requirements apply to all IT products and services such as computer equipment (including industrial machines with operating system), applications, hosting etc.

1. It is the Supplier's responsibility to ensure compliance of the goods and/or services with the applicable UTC security policy as per this IT requirements and any other requirements provided by PWRZ IT.

2. Hardware to be supplied:

· preferred configuration of a server, desktop computer, laptop or other computer equipment to be compliant with the current PWRZ standard (information available at any time from the PWRZ IT department);
· preferred operating system to be compliant with the current PWRZ standard (information available at any time from the PWRZ IT Department);
· the Supplier shall confirm legality (by providing a licence certificate, invoice) of each type of the installed and/or supplied software;
· the Supplier shall define details of the warranty conditions and support for the hardware delivered;
· PWRZ does not authorize the Supplier to remove any hard discs or any other information media used for testing and/or production purposes (with the system delivered) outside of the PWRZ company premises without prior written permission from PWRZ IT.

3. Access rights on the hardware delivered:

· Supplier has access rights to configure the device only to the point of final acceptance of the project/device. Any access privileges to perform service/support activities after final acceptance of the project/device have to be approved by PWRZ IT dept. during the final acceptance of the device / project, etc. the Supplier shall provide all the access rights, passwords, etc. to the systems and applications delivered as part of the assignment, order, etc.;
· such rights shall be transferred in writing in a sealed envelope to the representative of PWRZ IT department against confirmation of receipt;
· the Supplier shall not receive any rights of a privileged user (administrator, root, etc.) with regard to the delivered hardware during its use in the production process. Such rights may only be granted temporarily in a case of a justifiable need for a support/configuration or similar service performed by the Supplier, and only after prior PWRZ IT department approval.

4. Remote connection to the PWRZ computer systems shall at all times be subject to the following conditions:

· the Supplier shall make a written statement confirming its acceptance of the Non-Disclosure Agreement, which is a pre-requisite for commencement of cooperation;
· the Supplier acknowledges, undertakes and agrees that it is granted access to the PWRZ

computer systems only for the duration of the Agreement;
· the Supplier shall comply with the export control conditions relating to the transferred data (if applicable).
· the Supplier confirms that for remote connections it uses secure communication channels;

5. PWRZ reserves the right to refuse the Supplier's employees access to the PWRZ IT system, modem and/or network card connection to an external network, external link, phone line, etc. if the foregoing conditions are not met.

6. If application prepared for the purpose of PWRZ is subject of the Agreement source code used to creation of such application shall become PWRZ property. The Supplier shall provide source code of any systems or applications that are developed for PWRZ. PWRZ shall have the right to use, copy and modify provided source code. .

7. The Supplier confirms that it has appropriate legal rights to the tools and the software used in development of the goods and/or services for PWRZ under the Agreement.

8. The Supplier shall indemnify PWRZ against any claims that the development of the goods and/or services in any way infringes the intellectual property rights of a third party.

9. If the Agreement provides for development and/or modification of a website, then:

· the content published on the website shall be protected by copyrights; such rights are vested in PWRZ. The implementation and use of any tools for content search must be compliant with the UTC security policy. If the tools used for content search create copies of the source data, all the copies are subject to the same level of protection as the source data;
· the Supplier shall ensure regular updates of the website with PWRZ data through an electronic interface. Defining the scope of data and frequency of updates is the responsibility of PWRZ.

10. All the applications must use authorization and access control tools or they must have a functionality implemented ensuring their security and compliance with the UTC security policy, including:

· the passwords of the computer system users must have adequate level of complexity; system shall not accept any simple passwords eg. words similar to the user ID, characters ordered in the keyboard sequence (e.g. 123456, asdfgh), common acronyms etc;
· system shall be configured in such a way that passwords must be composed of at least 8 characters and must be changed at least every 60 days;
· passwords must be complex (contain characters from at least three different groups listed: special characters, lowercase letters, uppercase letters, alphanumeric characters);
· for service and communication IDs (“service IDs”) passwords must be composed of at least 15 characters;
· minimum password age is 1 day; passwords should be reused only after 6 months or at

least the last 5 passwords shall be recorded and not allowed to be reused
· passwords must not be displayed or stored in any open (unencrypted) file;
· User ID's that have not been used in the last three months shall be automatically locked out; after 1 year of inactivity user accounts are manually deleted.

11. Protection & security of PWRZ data stored within Supplier's IT systems:

· If, as a part of the Agreement, the Supplier maintains and/or processes any non-public PWRZ data (such as eg. personal, financial or technical data) then the Supplier must provide a copy of its current security policy of data storage and processing as well as its policy on physical access to the equipment used for storing and/or processing of the PWRZ data. Once in a year, the Supplier shall provide PWRZ with its up-to-date security policy.
· It is required that the Supplier should segregate the PWRZ data, keeping the data in separate databases accessible only by PWRZ, authorized parties and the Supplier's employees responsible for maintaining a particular environment.
· Supplier confirms that access to PWRZ data will be granted only to employees with no criminal record.
· The Supplier is responsible for providing protection against unauthorized access to PWRZ data.
· PWRZ data must have provided backup process throughout the term of the Agreement. The minimum requirements are: incremental backups every 24 hours and a full backup every 7 days. Backup copies shall be kept for at least 30 days.
· PWRZ or a third party indicated by PWRZ shall have the right to conduct a security audit at the Supplier's site without any prior notice. If the PWRZ data is stored in a shared environment, PWRZ may contract a third party to conduct such audit. The audit may cover any facilities and equipment used to store PWRZ data, including backups of such data and may verify if all the required controls have been implemented in line with the UTC security policy.
· Failure of audit of the data security & compliance as set forth in this requirements can be the basis for termination of the Agreement with the Supplier. PWRZ may indicate identified "soft spots" to the Supplier and the Supplier shall within 30 days provide PWRZ with a plan to remove such vulnerabilities and if PWRZ so requires, the Supplier shall apply interim solutions until all the vulnerabilities are removed. If the risks identified by PWRZ are not removed within the stated period or if the Supplier refuses to remove those vulnerabilities, PWRZ may terminate the Agreement forthwith.
· According to the UTC data security policy, any proprietary information transferred via public networks (such as the Internet) must be encrypted. The encryption technologies used shall be approved by PWRZ IT and shall comply with the applicable laws. The Supplier accepts the fact that non-public data will be transferred from PWRZ in an encrypted form if send eg. via email, as per current UTC encryption standards.
· Before or at the date of execution of the Agreement, the Supplier shall provide PWRZ with a plan which outlines how all the data, including its backups and archived data will be transferred to PWRZ upon termination or expiry of the Agreement and how that data will be permanently deleted from the Supplier's system. The plan must provide for the data to be delivered to PWRZ in a database (file format) compliant with the PWRZ

standards or else the Supplier shall deliver to PWRZ a licence for relevant software that will allow PWRZ to use the delivered data.
· the Supplier confirms that it has adequate procedures and safeguards in place against known data security threats (eg. Supplier uses and frequently updates antivirus software, is able to detect hacking attempts targeting Supplier's IT systems, etc);
· The Supplier is obliged to inform PWRZ of any third party attempts to acquire PWRZ data and/or any hacking attempts to Supplier's IT system.

12. The Supplier shall ensure updates of its procedures in case of an update in the UTC information security policies to provide compliance with the updated UTC policies.

13. Each external user shall follow all the policies and standards of PWRZ/UTC. The Supplier shall operate an awareness-building program on data security.

14. PWRZ reserves the right to assess the Supplier's capability to meet the UTC security policy requirements. The Supplier is obliged to present, at PWRZ's request, written confirmation, on how the above requirements are met.