Notes on IT baseline protection for computers of guests of the Research Centre Jülich

The IT-Security Guideline (http://intranet.fz-juelich.de/SharedDocs/Downloads/IT-PORTAL/DE/IT_Security/IT%20Security%20Guideline%20-%20English.html) of the Research Centre, as issued by the Board of Directors, commits the administrators and users of all IT-systems in the Research Centre to actively contribute towards the important goal of ensuring adequate IT security. This includes in particular to obey the IT Security Rules for Baseline Protection (http://intranet.fz-juelich.de/SharedDocs/Interne_Regelungen/IT_Security_Rules_for_Baseline_Protection_IR_119-1.html). This also applies to computers of guests which connect to JuNet. The following notes summarise rules which are especially important for guests. They are intended as an introduction and by no means substitute the IT Security Rules for Baseline Protection.

1. Connection to JuNet:

1.1 **Registration**

Each computer must be registered (https://junet-portal.fz-juelich.de/cgi-bin/public/start_junet.cgi) at JSC and have an appointed administrator who is an employee of the Research Centre and who has acknowledged the IT Security Rules for Baseline Protection.

1.2 **Security Ceckup**

Before being attached to JuNet, the state of IT security of a computer has to be inspected (current patches, virus-scanner, check for viruses). The check covers:

- making the operating system „network-proof“ (minimum requirements for patch-level)
- if not already present: installation of an automatically updating virus-scanner
- an Online-Update of Windows- and if possible also Linux-systems

2. System Configuration:

2.1 **Password protection and access**

All accounts on the computer have to be protected by a non-trivial password. Privileged accounts (Administrator, root) may only be accessible via networks if strong encryption is used (e.g. via ssh).

2.2 **Operating System and Applications**

Security parameters offered by the operating system and applications should be used (e.g. personal firewalls, secure configuration of web-browsers and email-clients).

2.3 **Network Configuration**

The computer must be configured such that is does not communicate in JuNet and W-JuNet at the same time. (Otherwise it could open a side path into JuNet.)

3. **Further Rules of Conduct:**

3.1 **Cautiousness**

Act with appropriate cautiousness when using the network: don’t open email attachments of unknown senders; remember that email-sender addresses can easy be faked; don’t install software from unknown or dubious sources; avoid visiting web-sites with dubious content.

3.2 **In Case of an Emergency**

In case of any suspicious behaviour please contact the FZJ-CERT via phone 02461 / 61-6440 immediately. This is inevitable to initiate appropriate counter-measures and thus prevent a possible larger damage for the Research Centre. After contacting FZJ-CERT you will be adviced to provide further detail information. Please do not collect any information in advance, since this could warn potential hackers. Please always first contact FZJ-CERT.

FZJ-CERT, October 2017