Granting local administration rights

on Linux hosts of the provider *science+computing* (s+c) at MBRDNA/DGRC RD

Granting local administration rights for individual users requires acknowledgement and agreement of the following obligations.

The devices and software provided by Daimler for information processing as well as the data stored on these devices are meant solely for professional and professionally initiated purposes.

The user acknowledges that by being granted local administration rights he provides a non-standard host and is therefore only entitled to a restricted support. These administration rights are granted only for one host. The local administration rights can be withdrawn at any time. The IO (Information Officer) reserves the right to withdraw the user's administrations rights granted so far upon violation of these obligations. The administration rights are granted for the current calendar year and their necessity is examined after the end of the calender year by the coordinator/decision maker of the technical division. The provider together with the Daimler representative maintains an appropriate list.

The user explicitely agrees to observe the following points:

Security/Operational Safety

(1) System configuration: No changes must be made to the defined LDAP/AD connection. The defined local administration rights must not be changed or deleted. Dissemination of local administration rights to other persons is forbidden. It is not allowed to create new users and user groups or to change the user's group affiliation. Changes of the configuration of the basic software distribution (package administration system) are not allowed. Regarding the installation of additional software, see (7).

(2) It is not allowed to make any changes to the virus scanner (currently Sophos) and to its configurations.

(3) It is not allowed to disable, delete or stop any service of the standard installation. If a service has to be stopped in certain application cases, the host must be disconnected from the official Daimler network.

(4) It is not allowed to provide network services that are relevant for the network operation, e.g. BootP, BootP Relay, DHCP, DHCP Relay.

(5) It is not allowed to enable routing functionalities on the host, e.g., proxy functionalities, IP routing, NAT.

(6) It is not allowed to use software (sniffer) to record, detect and protocol network traffic in the productive network. This also applies to so-called hacking tools for the manipulation of software, systems and user IDs.

(7) By the installation of additional software, hardware components and hardware drivers, no security risks must arise that may threaten or compromise the IT operation. The user must keep individually installed software, including hardware drivers up-to-date, and is obliged to install released security updates (patches) according to corporate policies (e.g., Daimler Information Security Compendium DISC, http://intra.corpintra.net/intra-itm-s/disc-de).

Licensing and Copyright Law

(8) The applicable licencing and copyright law of the used software must be observed.

(9) Concerning commercially used software installed by the user, the user himself must ensure its proper licensing. This also applies for software that may be used commercially according to its licensing terms, for which, however, no license fees are caused (freeware).

(10) It is forbidden to install and operate software with license obligation that has not been licensed by Daimler AG. Exception is software described by point 11.

(11) Downloading software from the Internet (e.g., via exchange platforms) may cause copyright infringement and is therefore explicitly prohibited. Exceptions are freeware, patches, drivers, trial versions and already licensed software officially provided by the software manufacturer (e.g., for evaluation reasons or update).

(12) Software installations (also updates and other changes relevant for licensing) must only be executed if they do not violate applicable licensing law.

(13) Concerning software with license obligation installed by the user, a license must be demonstrated to the IO (Information Officer) on demand.

Guidelines and Data Security

(14) The currently effective password rules must be obeyed. Find them in the Daimler Information Security Compendium DISC, Chap 3.1 „Password“ and Chap. 3.1.1 (http://intra.corpintra.net/intra-itm-s/disc-de) as applicable document of the Information Security Guideline A21 in the Einheitlichen Regelungsdatenbank (standard regulation database) ERD.

(15) It is not allowed to use the Internet with administrative user ID. Only if no other technical option is available, the administrative account may be used in exceptional cases.

(16) During analysis of system files, the data security regulations must be obeyed. (no personal data evaluation)

o I will **not** use Wireshark

o I will use Wireshark.
I know that Wireshark / WinPcap provides the possibility to record and analyze arbitrary network traffic. I herewith confirm using this kind of tools only for network traffic between my computer and car pcs / control units. Recording and analyzing network traffic between other computers or using Wireshark in the Daimler network (especially the RD network) is strictly forbidden and can cause personal consequences.

o additional admin user
I am informed that I should not save private data on the system since there is no data security because of multiple local admin rights.

For any further questions contact s+c at sc-cat-mbrdna@daimler.com.

I have read the information and agree.

User (please do not enter manually)
User ID: ______________________________
Name: ______________________________
First name: ______________________________
Hostname: ______________________________
Department: ______________________________
Date: ______________________________
Signature:

Approved by (E5)
Name: ______________________________
First name: ______________________________
Department: ______________________________
Date: ______________________________
Signature: