Der Fakultätsrat der Fakultät für Maschinenbau der Gottfried Wilhelm Leibniz Universität Hannover hat am 09.12.2020 in seiner Sitzung die folgende Nutzerordnung beschlossen.

Nutzungsordnung für die IT-Pools am Maschinenbau Campus Garbsen

Diese Nutzungsordnung soll das Miteinander in den IT-Pools am CMG regeln und ergänzt die Nutzungsbedingungen des LUH-Datennetzes – insbesondere die Nutzungsordnung der Leibniz Universität IT Services der Gottfried Wilhelm Leibniz Universität Hannover siehe dazu auch
https://www.luis.uni-hannover.de/fileadmin/it-support/Nutzungsordnung_LUIS-IT_2017-08-17.pdf

§ 1. IT-Geräte die sich nicht im Eigentum der Universität befinden

Es dürfen keine privaten Geräte ohne explizite Zustimmung des zuständigen Administrators an das Netz der Universität angeschlossen werden! Für den kostenfreien Internetzugang steht das WLAN der Leibniz Universität Hannover zur Verfügung. Accounts sind über https://login.uni-hannover.de zu erhalten. Die Nutzung des Stromnetzes in den Räumen der Leibniz Universität Hannover ist nur für Geräte gestattet, die im direkten Zusammenhang mit einer Lehrveranstaltung, Prüfung oder Studien-/Projekt-/Abschlussarbeit stehen. Der ordnungsgemäße Zustand und eine in Deutschland gültige Zulassung (CE/TÜV) sind vorher zu überprüfen und sicherzustellen.

§ 2. Zugang zu den IT-Pools

Die Weitergabe von Zugangsdaten/-mitteln wie Passwörtern, Schlüsseln bzw. Transpondern an Dritte ist strengstens untersagt und führt zur sofortigen Accountsperrung der Nutzenden. Evtl. notwendige Schlüssel- bzw. Transponderausgaben erfolgen über die zuständigen Mitarbeiter*innen des Instituts (Betreuende Person), welches die Notwendigkeit der Nutzung der Infrastruktur hat. Die notwendige Schließberechtigung wird durch den zuständigen Mitarbeiter*Innen dem Transponder hinzugefügt. Die Pools stehen im Regelfall während der Öffnungszeiten und außerhalb von Lehrveranstaltungen den Studierenden zur Verfügung. Vorrang vor jeder anderen Art von Nutzung haben immer Lehrveranstaltungen, welche auf eine IT-Infrastruktur angewiesen sind. Die Türen der Pool-Räume sind geschlossen zu halten. Personen ohne entsprechende Pool-Nutzungsberechtigung ist kein Zugang zu gewähren.

§ 3. Sauberkeit der PC-Pool-Räume / Verbot offener Getränke

(1) In den Pool-Räumen sind offene Getränke wie z.B. Kaffee und Tee untersagt. Getränke in verschlossenen Gefäßen/Flaschen dürfen mitgebracht und verzehrt werden.

(2) Flüssigkeiten und Speisen sind mindestens einen halben Meter von der IT-Infrastruktur entfernt zu halten. Pausenbereiche außerhalb der Pools sind bevorzugt für die Nahrungsaufnahme zu benutzen.

(3) Die Tische sind nach der Nutzung sauber zu hinterlassen. Eigenes Arbeitsmaterial ist zu entfernen und mitzunehmen oder ggf. beim betreuenden Mitarbeiter*Innen zu hinterlegen.

§ 4. Userprofile/Accounts

(1) Das Speichern **von Daten auf dem Benutzerprofil ist untersagt.** Ausnahme bildet das kurzzeitige Speichern von Daten während Lehrveranstaltungen oder zur Übertragung auf andere Medien, da es sonst beim An- und Abmelden zu langen Wartezeiten kommen kann (Profilsynchronisation). **Userdaten müssen immer auf einem Netzwerklaufwerk/Cloud abgelegt werden.** Die Zugangsmöglichkeit zur universitären Seafile-Cloud ist aus jedem Account möglich. Daten auf Benutzerprofilen können jederzeit ohne Information des Nutzenden gelöscht werden. Eine Sicherung der Daten wird nicht vorgenommen und obliegt dem Nutzenden.

(2) Die Zum Anlegen der Userprofile/Accounts zur Nutzung der CIP-Pools werden folgende personenbezogenen Daten verarbeitet und aus dem IdM der LUH übermittelt:

LUH-ID, UID, Fakultät, Zugehörigkeiten, Name, dienstespezifisches Passwort

Diese Daten werden solange gespeichert, wie der Account im IdM aktiviert bleibt. Bei Ausscheiden aus der Universität sorgt das IdM durch entsprechende automatisierte Benachrichtigung für eine automatisierte Löschung dieser o.g. und zugehörigen Daten. Bei längerer Nichtnutzung (>3 Monate) des Accounts behält sich die Systemadministration das Recht vor, darin gespeicherte Nutzdaten zu löschen.

(3) Einsicht in die o.g. Daten haben nur die zuständigen Systemadministrator*innen der Einrichtung, dessen Verwendung der Infrastruktur durch den Nutzenden beantragt wurde. Die IT-Verantwortlichen der Einrichtungen sind auf den Seiten der Leibniz Universität Hannover aufgeführt.

(4) Die Daten der Nutzenden können bei Vorliegen der gesetzlichen Voraussetzungen an Strafverfolgungsbehörden weitergegeben werden.

§ 5. Betrieb/Installation von Fremdsoftware

(1) Der Betrieb von nicht im Pool bereitgestellter Software sowie deren Installation ist nicht erlaubt.*

(2) Die Systemadministratoren haben das Recht alle Daten auf der lokalen/Pool IT-Infrastruktur einzusehen um Missbrauch zu erkennen. Insbesondere urheberrechtlich geschütztes Material (Musik, Filme, E-Books ohne wissenschaftlichen Bezug) wird ohne weitere Vorankündigung von den Rechnern entfernt und bei Verdacht auf Vorliegen einer Straftat ggf. den Strafverfolgungsbehörden gemeldet.

§ 6. Nutzung der Infrastruktur zu nicht Studienzwecken

Das Ausspionieren und Eindringen in Fremd-Rechner, -Netze, sowie die vorsätzliche Verbreitung von Schad- oder Spionagesoftware ist strengstens untersagt. Darüber hinaus ist auch die Nutzung von Seiten bzw. Dateien mit strafrechtlich relevanten Inhalt oder das Vorhalten bzw. Abspielen dieser mithilfe der IT-Infrastruktur der Pools nicht erlaubt. Dies betrifft insbesondere den Download von sog. Warez, KeyGens und Tools zum Umgehen von Kopierschutzmaßnahmen. Die Vorgänge werden mit der Sperrung des Accounts geahndet. Weiterhin werden die Daten forensisch gesichert und die Tat unverzüglich zur Anzeige gebracht.

§ 7. Inkrafttreten

Diese Ordnung tritt mit dem Tage nach ihrer hochschulöffentlichen Bekanntmachung in Kraft.

Beim Verlassen der Räumlichkeiten sind die PCs herunterzufahren* und die Monitore ebenfalls abzuschalten. Fenster und Türen sind beim Verlassen der Räume abzuschließen. Den Anweisungen des Personals vor Ort ist in jedem Fall Folge zu leisten.

*** Vereinzelte Ausnahmen von dieser Regel sind nach Absprache mit dem zuständigen Systemadministrator*in möglich.**