

Betriebsregelung für das Datennetz UKLAN der Universität zu Köln (UKLAN-Betriebsregelung)

(<http://www.uni-koeln.de/rrzk/uklan/betriebsregeln/>)

- 1 Einordnung
- 2 Begriffsbestimmungen und Anschluß von Geräten
- 3 Verpflichtungen des RRZK
- 4 Verpflichtungen der Benutzer
- 5 Technische Detailregelungen

Die nachfolgend wiedergegebene und vom Regionalen Rechenzentrum in Ergänzung der Benutzungsordnung erlassene Betriebsregelung basiert weitgehend auf einem Entwurf, der aus dem Arbeitskreis der Leiter Wissenschaftlicher Rechenzentren (ALWR) hervorging. Sie tritt zum 1. Januar 1993 in Kraft.

Bei Fragen zur UKLAN-Betriebsregelung wenden Sie sich bitte an Herrn Claus Kalle (E-Mail: Kalle@rrz.Uni-Koeln.DE).

1 Einordnung

- Das Datennetz UKLAN ist eine zentrale, nachrichtentechnische Infrastruktureinrichtung der Universität zu Köln. Es dient der allgemeinen Datenkommunikation und ist anderen Infrastrukturmaßnahmen, wie z.B. Elektrizitätsversorgung, Wasserversorgung oder Telefon gleichgestellt. Es wird vom Rechenzentrum der Universität zu Köln, zugleich Regionales Rechenzentrum (im folgenden mit RRZK bezeichnet) im Sinne der Grundordnung der Universität zu Köln vom 23. Oktober 1990 und der Benutzungsordnung vom 29. Januar 1992 betrieben.
- Das Datennetz UKLAN ist eine komplexe technische Einrichtung, die nur bei hohen Anforderungen an die Sorgfalt und das Wissen geplant, installiert, betrieben, gewartet und repariert werden kann. Daher wird diese Betriebsregelung nach Paragraph 5 Ziffer 1 der Benutzungsordnung des RRZK erlassen. Sie tritt am 1. Januar 1993 in Kraft.

2 Begriffsbestimmungen und Anschluß von Geräten

- Das Datennetz UKLAN umfaßt alle Übertragungseinrichtungen (Kabel, Vermittler, usw.) einschließlich der Anschlußpunkte für Endgeräte. Ausgenommen davon sind Übertragungseinrichtungen in der Zuständigkeit anderer Stellen (z.B. das Telefonnetz). Das Datennetz UKLAN beruht auf den Standards IEEE 802.3 (Ethernet), IEEE 802.5 (Token Ring) und ANSI X.3 T95 (FDDI). Das Datennetz UKLAN hat Verbindungen zum internationalen Internet, zum nationalen Wissenschaftsnetz WiN und zu öffentlichen Netzen.
- Das Datennetz UKLAN wird einschließlich der Anschlußpunkte im Rahmen der verfügbaren zentralen Mittel bereitgestellt und betrieben. Die dazu in angeschlossenen Rechnern notwendigen Hard- und Softwarekomponenten sind von dessen Betreiber zu finanzieren.
- Das Datennetz UKLAN erlaubt durch Einsatz geeigneter Kopplungseinrichtungen (z.B. Multiprotokollrouter) eine Strukturierung und bietet dabei eine transparente, wahlfreie und leistungsfähige Kommunikation aller Teilnehmer untereinander. Von Einrichtungen selbständig betriebene Netze, die am Übergabepunkt z.B. durch Multiprotokollrouter an das Datennetz UKLAN angekoppelt werden können, sind nicht Teil dieses Datennetzes. Auf Multiprotokollrouter kann nur verzichtet werden, wenn der für die Ankoppelung Verantwortliche nachweist, daß der Netzbetrieb nicht gestört wird, daß für das RRZK keine nennenswerte Mehrbelastung entsteht, und daß keine Hard- oder Software eingesetzt wird, die geeignet wäre, den Informationsfluß im Datennetz UKLAN zu beobachten, mitzulesen oder zu beeinflussen.
- Kommunikation ist nur möglich, wenn die eingesetzten Protokolle bei Sender und Empfänger gleich sind. Die Protokollvielfalt ist auf das unbedingt notwendige Maß zu begrenzen, damit die Kommunikation technisch erleichtert und die Komplexität so gering wie möglich gehalten wird. Insbesondere ist die Verwendung unterschiedlicher Protokolle für vergleichbare Lösungen zu vermeiden. Unter Umständen können Netze entstehen, die wie unter 2 c selbständig betrieben werden müssen und über Multiprotokollrouter mit dem Datennetz UKLAN verbunden werden können.
- Der Anschluß von Rechnern oder anderen Endgeräten, die vom Nutzer korrekt zu konfigurieren sind, erfolgt auf Antrag durch das RRZK im Rahmen der technischen Möglichkeiten. Änderungen (z.B. Austausch des Rechners) müssen dem RRZK gemeldet werden.

- Die Anschlußpunkte dürfen nur vom RRZK eingerichtet oder verändert werden. Rechner dürfen nur an den Anschlußpunkten betrieben werden, für die eine Nutzungserlaubnis besteht.
- Wird der Netzbetrieb über einen Anschlußpunkt oder ein angeschlossenes Endgerät gefährdet, unzumutbar behindert oder gestört, so kann das RRZK geeignete Auflagen machen oder die Anschlußstrecken stilllegen.
- Die für die Nutzung angegebener Netze (z.B. Internet/NSFnet) bestehenden Regeln (z.B. NSFnet acceptable use policy) müssen befolgt werden. Bei Mißachtung dieser Regeln kann das RRZK geeignete Auflagen machen, oder die Anschlußstrecken von der Nutzung dieser Netze ausschließen. Eine aktuelle Version dieser Regeln ist auf Anfrage beim RRZK erhältlich.

3 Verpflichtungen des RRZK

- Das RRZK ist verpflichtet, einen sicheren und möglichst ununterbrochenen Netzbetrieb zu gewährleisten. Nicht vermeidbare Störungen sind auf ein Minimum zu beschränken.
- Das RRZK vergibt die Netzwerkadressen, ist für das Netzwerkmanagement zuständig, berät in Fragen der Nutzung des Datennetzes UKLAN und sorgt für eine Dokumentation des Netzes und seiner Nutzungsmöglichkeiten.
- Die verfügbaren und einsetzbaren Netzdienste und Protokolle werden vom RRZK bekanntgemacht. Zusätzliche, andersartige Protokolle werden mit Zustimmung des RRZK nur in Ausnahmefällen für einen eingrenzbaeren Einsatz zugelassen. Anfallende Kosten gehen dabei zu Lasten der die Ausnahme beantragenden Einrichtung, die auch dafür zu sorgen hat, daß der übrige Netzbetrieb nicht gestört wird. Diese Regelung betrifft speziell nicht routbare Protokolle (z.B. DEC LAT).
- Das RRZK übernimmt keine Verantwortung für Beeinträchtigungen, die über das Datennetz UKLAN an die angeschlossenen Rechner herangetragen werden.
- Das RRZK hat dafür Sorge zu tragen, daß nur seine besonders ausgewiesenen Mitarbeiter bei Fehlererkennung, Fehlerverfolgung und Netzverwaltung eingesetzt werden.

4 Verpflichtungen der Benutzer

- Für jeden an das Datennetz UKLAN angeschlossenen Rechner ist dem RRZK ein technisch Verantwortlicher zu benennen.
- Bei der Übermittlung von Daten ist zu beachten, daß Dritte insbesondere durch Mißbrauch mithören könnten. Der Benutzer hat bei der Datenübertragung die Datenschutzgesetze zu beachten. "Mithören", Ausspionieren, Aufzeichnen sowie Verändern fremder Daten aus dem Datennetz UKLAN sowie das Stören der Kommunikation sind verboten. Davon ausgenommen sind Maßnahmen der Fehlerverfolgung durch das RRZK. Benutzer oder Dritte dürfen keine Modifikationen am Datennetz UKLAN vornehmen. Identifikationsmerkmale von Rechnern (Netzadressen, Namen, usw.) dürfen nur in Absprache mit dem RRZK verändert werden.
- Bei den an das Datennetz UKLAN angeschlossenen Rechnern obliegt der Schutz vor unberechtigtem Zugang und unberechtigtem Zugriff auf gespeicherte Daten dem jeweiligen Rechner-Betreiber. Der Benutzer darf aus dem Datennetz UKLAN nur diejenigen Daten auf seinen Rechner leiten, die für ihn bestimmt sind. Beschaffung und Einsatz von Hard- und Software, die einen Mißbrauch ermöglichen, sind unzulässig.
- Der Benutzer ist verpflichtet, dem RRZK Unregelmäßigkeiten, Störungen oder Mißbrauchsversuche anzuzeigen.
- Der Datenverkehr eines Benutzers darf den anderer Benutzer nicht unangemessen beeinträchtigen. Der Einsatz besonders netzbelastender Übertragungen ist mit dem RRZK abzustimmen.
- Das Datennetz UKLAN darf nicht zur Überwachung oder Leistungskontrolle von Mitarbeitern verwendet werden.
- Ein Verstoß gegen diese Betriebsregelung gilt unbeschadet weitergehender Gesetze (z.B. in Analogie zum Fernmeldegesetz) auch als Mißbrauch im Sinne der Benutzungsordnung des RRZK.

5 Technische Detailregelungen

Technische Detailregelungen werden vom RRZK erstellt und dem Bedarf entsprechend fortgeschrieben.

Zusatz: Identifizierbarkeit der Benutzer

Alle Benutzer mit Zugang zum Internet müssen durch einen eindeutigen Usernamen und Passwortschutz identifizierbar sein. Falls aus irgendwelchen Gründen anonyme Accounts unumgänglich sind, müssen Vorkehrungen getroffen werden, die verhindern, daß von dort aus Eingaben im Netz verbreitet werden können.

Regelungen für den Betrieb von Rechnern am lokalen Netz der Universität zu Köln (UKLAN)

(Ergänzung zur UKLAN-Betriebsregelung)

In der letzten Zeit ist das lokale Netz der Universität zu Köln UKLAN (Universität zu Köln Local Area Network) weiter gewachsen. Mit diesem Wachstum werden auch immer mehr Rechner am UKLAN betrieben. Um wie bisher einen störungsfreien und sicheren Betrieb des Netzes und der an ihm angeschlossenen Systeme zu gewährleisten, wurde vom RRZK in der Abteilungsleitersitzung vom 7. Februar 1995 die hier wiedergegebene Betriebsregelung verabschiedet, die die bestehende [UKLAN-Betriebsregelung](#) vom 1.1.1993 (veröffentlicht im RRZK-Kompass Nr. 56, S. 28 ff.) ergänzt. In ihr sind die wesentlichen, bereits lange praktizierten Absprachen schriftlich niedergelegt.

Um einen gesicherten und verlässlichen Betrieb des lokalen Netzes der Universität zu Köln (UKLAN) und der an ihm angeschlossenen Rechner, auch im internationalen Netzwerk Internet, zu gewährleisten, ist es notwendig, Regelungen zur Konfiguration und zum Betrieb von Rechnersystemen am UKLAN zu beachten.

Die Einrichtungen und Institute der Universität sind verpflichtet, diese Regelungen dringend einzuhalten. Eine Mißachtung kann nicht nur zu Betriebsstörungen, sondern im schlimmsten Fall zu externen Forderungen an die Universität zu Köln führen. Das Rechenzentrum behält sich vor, jederzeit die Einhaltung dieser Regeln, ggf. stichprobenartig, zu überprüfen. Die Nichtbeachtung dieser Regeln kann zum sofortigen Entzug der UKLAN-Verbindung für das betroffene Teilnetz führen, womit das RRZK dann größeren Schaden, auch im Interesse des Rechnerbetreibers, vermeiden hilft.

- Die jeweils aktuellen Internet-Standards mit dem Titel "Requirements for Internet Hosts" (z. Zt. RFC 1122 und RFC 1123 bzw. STD 3) müssen erfüllt sein.
- Auf den am UKLAN betriebenen Systemen dürfen keine Gast-Zugänge und keine Zugänge ohne Paßwort eingerichtet werden. Am UKLAN betriebene Rechner dürfen nur zu Zwecken der Forschung und Lehre bzw. zu dienstlichen Zwecken genutzt werden. Dabei sind die Benutzer durch gängige Verfahren (z.B. login mit Paßwort, Ausweise bei PC-Nutzung) zu authentifizieren.
- Auf Mehrbenutzer-Systemen sollen neben der üblichen sicherheitstechnischen Konfiguration regelmäßige Überprüfungsläufe mit entsprechender Software gefahren werden (z.Zt. ist dies für Unix etwa das Paket COPS der Purdue-University).
- Die Benutzer sind mit geeigneten Maßnahmen dazu anzuhalten, auf Mehrplatzsystemen nicht-errätbare Paßworte zu verwenden (z.Zt. etwa durch regelmäßige Überprüfung der Ratbarkeit von Paßworten mit dem Tool CRACK).
- Die Inanspruchnahme von externen Netzdiensten wie etwa dem Zugriff auf externe Dateiserver mit ftp oder die Nutzung von Informationsdiensten (www/gopher) oder netnews soll koordiniert mit den durch das RRZK lokal vorgehaltenen Diensten geschehen. Dadurch kann z.B. unnötiger Doppelbezug von Dateien und Nachrichten vermieden werden.
- Das Angebot von Netzdiensten nach außen soll mit dem RRZK abgestimmt werden. Dabei übernimmt das RRZK die Rolle einer Clearingstelle, um Kollisionen und Doppelangebote zu vermeiden.
- Das RRZK wird spezielle Dienste, die besonders auf die Möglichkeiten und Erfordernisse der vom RRZK betriebenen Servermaschinen (z.B. die Verfügbarmachung von Home-Directories mit NFS, der Betrieb von AFS-Fileservern der RRZK-Zelle) abgestimmt sind, aus Sicherheitsgründen nur in besonderen Ausnahmefällen auf nicht vom RRZK betriebenen Rechnern verfügbar machen.
- Allgemein sind die vom RRZK vermittelten Konfigurationsrichtlinien zu beachten. Diese werden z.B. in den entsprechenden Systemverwaltungskursen der Abteilung Systeme, in

Betriebsregelungen und Anleitungen auf dem ftp-Fileserver des RRZK, im Benutzerleitfaden und in der Hauszeitschrift des RRZK, RRZK-Kompass, dargestellt.

Das RRZK versucht nach Möglichkeit, die Institute bei der Gestaltung ihrer Konfiguration und ihrer betrieblichen Einbettung zu beraten. Erste Anlaufstelle für Fragen und Hilfestellung zu dieser Anleitung ist die Beratung des RRZK oder der für das Institut zuständige Fachbereichsbetreuer.

Diese Regelung tritt sofort bei Bekanntmachung in Kraft.

Köln, den 3. Januar 1995

Gez. Claus Kalle, Ltg. Abteilung Systeme

(Quelle: <http://www.uni-koeln.de/rrzk/uklan/betriebsregeln/rechner.html>)

Schutz der UKLAN-Subnetze

Ab

1.1.1999:

Standardmäßig kein Zugang aus dem Internet in Institutsnetze

Um für UKLAN-Subnetze in der Universität standardmäßig einen verbesserten Schutz gegen Angriffe aus dem Internet zu implementieren, haben wir in der 23. und letzten Sitzung der Senatskommission für das Rechenzentrum am 13.02.1998 ein geeignetes Verfahren vorgestellt, das die Kommission befürwortet hat. Im Kurs 13 des Herbstkursangebots des ZAIK zum Thema „Security beim Betrieb von Rechnern am UKLAN“ bestand unter den anwesenden Systemverantwortlichen gleichfalls Übereinstimmung, daß Maßnahmen zum standardmäßigen besseren Schutz von UKLAN-Subnetzen wünschenswert sind. Mit dem Ausbau der Netztechnik im Laufe dieses Jahres bekommen wir technisch die Möglichkeit, dies Verfahren nun auch mit Wirksamkeit zum 1.1.1999 zu realisieren.

Ab 1.1.1999: Standardmäßig kein Zugang aus dem Internet in Institutsnetze Ab 1.1.1999 gilt, daß Rechner in einem UKLAN-Subnetz (Institutsnetz) standardmäßig nicht mehr von außen aus dem Internet erreicht werden können. Umgekehrter Verkehr, also die Nutzung von im Internet angebotenen Diensten aus dem Institutsnetz, bleibt von dieser Regelung unbeeinflusst. Insofern wird also die konsumptive Nutzung des Internet-Angebots nicht beeinflusst.

Anders verhält es sich mit Diensten, die aus dem Institutsnetz nach außen angeboten werden sollen. Dies könnte z.B. Dialogzugang mit telnet zu einem großen Institutsserver betreffen oder auch einen ftp-Server, der Dateien zur Nutzung aus dem Internet anbietet. Dieses Dienstangebot muß beim RRZK registriert werden, um die Netztechnik so konfigurieren zu können, daß die Möglichkeit der Nutzung der bezeichneten Institutsressourcen (technisch gesprochen Rechneradressen und TCP- bzw. UDP-Portnummern) von außen erhalten bleibt.

Darüber hinaus denkbar ist der Fall, daß ein Institut wünscht, komplett von dieser Maßnahme ausgenommen zu werden und weiterhin alle im UKLAN-Subnetz betriebenen Rechner mit vollem aktiven und passivem Internet-Zugang verbunden wissen möchte. Diese risikoreichste Betriebsart sollte mit Bedacht nur bei entsprechender Qualifikation der Betreuer zur Rechner- und Netzpflege gewählt werden.

Zur Erinnerung: Schon seit dem Oktober 1997 ist ja im Rahmen der notwendigen Anti-Spam-Maßnahmen der Betrieb von Email-Server-Systemen in den Subnetzen des UKLAN nur noch kontrolliert erlaubt.

Um die Absichten eines UKLAN-Subnetzverantwortlichen (dies ist letztlich der betreffende Institutsdirektor) bzgl. Ausnahme von der ab 1.1.1999 geltenden Regelung zu erklären, wurde das auf der nächsten Seite wiedergegebene Formular entworfen. (*Anmerkung der Redaktion: Das Formular ist hier nicht wiedergegeben sondern als Acrobat-Datei/pdf-Datei unter der URL <ftp://ftp.rrz.uni-koeln.de/rrzk/antraege/uklan-subnetz-schutz.pdf> abgelegt.*) Wir bitten dieses ggf. bis zum 15.12.1998 auszufüllen, zu unterschreiben und per Hauspost an das

RRZK

z.Hd. Herrn Liebchen

einzusenden. Nur beim rechtzeitigen Eintreffen können wir für den störungsfreien Weiterbetrieb Ihrer nach außen angebotenen Services im Instituts-Subnetz sorgen! Falls Sie sich dem Standard anschließen wollen und das Internet in Zukunft nur konsumtiv nutzen wollen, ist keine Reaktion notwendig. Zum 1.1.1999 werden wir ihr Subnetz dann (soweit technisch möglich) schützen.

Schlußbemerkung: Mail-Server, die uns bereits formlos im Rahmen der Anti-Spam-Maßnahmen mitgeteilt wurden, brauchen hier nicht erneut aufgeführt zu werden. Falls jedoch einmal Änderungen in Ihrem Service-Angebot auftreten, bitten wir um vollständige Mitteilung aller Ihrer Services. Bitte bewahren Sie daher eine Kopie Ihrer Mitteilung an uns auf.

Claus Kalle

(Quelle: <http://www.uni-koeln.de/rrzk/uklan/betriebsregeln/subnetze.html>)