Richtlinien
zur Nutzung der EDV/IT-Infrastruktur am EWZ

1. Gegenstand der Richtlinien

Die folgenden Richtlinien regeln die Nutzung der IT-Infrastruktur am EWZ. Diese Infrastruktur umfasst sowohl die zur Verfügung gestellten IT-Dienste (z. B. Internet-Zugang, Mail, File- und Printservices, etc.) als auch die Ausstattung der IT-Räume (IT001, IT003), die zur Verfügung gestellten kabelbasierenden und drahtlosen Netze, die Arbeitsstationen in der Bibliothek, die Medienausstattung und Vortragsrechner in den Hörsälen, Seminar-, Gruppen- und Praktikumsräumen, sowie die Arbeitsstationen der Mitarbeiter und das jeweilige Zubehör.

2. Nutzung und Obliegenheiten des Nutzers

Die Nutzung der gesamten IT-Infrastruktur ist ausschließlich im Rahmen der Tätigkeit am EWZ bzw. für studienbezogene oder wissenschaftliche Zwecke zulässig.

Der Nutzer ist verpflichtet, sorgsam und verantwortungsvoll mit der genannten IT-Infrastruktur umzugehen. Insbesondere hat der Nutzer jegliche nicht genehmigte Veränderung der IT-Infrastruktur (Hard- und Software) zu unterlassen. Fehlfunktionen, Beschädigungen oder Verlust sind unverzüglich der IT-Abteilung des TCC zu melden. Schäden an der IT-Infrastruktur, die mutwillig oder grob fahrlässig verursacht werden, ziehen Schadensersatzansprüche nach sich. Vorsätzliche rechtswidrige oder missbräuchliche Verwendung ist streng untersagt und wird verfolgt.

3. Besondere Richtlinien für Mitarbeiter-PCs

Es gelten alle Richtlinien unter Punkt 2. Grundvoraussetzung für den Anschluss einer Arbeitsstation an das TCC-Netz ist die Installation des vom TCC verwendeten Virenschutz-Produktes. IT-Service jeglicher Art wird von der TCC-IT-Abteilung nur dann erbracht, wenn die betreffende Arbeitsstation über das TCC angeschafft wurde und die vorgegebenen Serviceagenten bzw. das gültige Standard-Betriebssystemimage installiert sind. Ein Network-Access-Controlsystem überwacht die am TCC-Netz angeschlossenen Geräte und deaktiviert ggf. den Anschluss nicht-konformer Arbeitsstationen. Die TCC-IT-Abteilung hat die Möglichkeit, mit Einwilligung des Nutzers per Fernwartung auf seine Arbeitsstation zu Servicezwecken zuzugreifen – mit Anmeldung am TCC-Netz erklärt sich der Nutzer mit dieser Vorgangsweise einverstanden. Eigene Software-Installationen sowie Hardwareumbauten sind nur nach Rücksprache mit der TCC-IT-Abteilung zulässig. Eine Nichtbeachtung dieser Regelung zieht den Verlust des IT-Services durch die TCC-IT-Abteilung nach sich. Für Sonderkonfigurationen, die vom TCC-Standard abweichen, wird die gesetzliche Gewährleistung übernommen, jedoch kein IT-Service geleistet.

4. Besondere Richtlinien für Vortrags-PCs und Medienausstattung in Hörsälen & Seminarräumen

Es gelten alle Richtlinien unter Punkt 2. Lehrpersonen können Dateien zum Zwecke der Präsentation auf den jeweiligen Vortragsrechner übertragen und auf diesem starten. Möglich ist dies mit Dateien des Typs Adobe™ Acrobat™ sowie den Dateiformaten von Microsoft™ Office ™ (in der aktuell eingesetzten Version) für Windows ™ und den gängigen Bilddateiformaten. Die Darstellung davon abweichender Formate kann nicht garantiert werden. Alle Vortragsrechner werden in unregelmäßigen Abständen und ohne Ankündigung oder Rücksprache von der TCC-IT-Abteilung neu installiert und sind somit nicht als Datenablage zu verwenden. Nach Abschluss der Lehrveranstaltung ist der Rechner herunterzufahren und der Beamer bzw. die genutzten Medien ggf. mit der dafür vorgesehenen Taste am Medienswitch bzw. Bedienpanel auszuschalten. Dies gilt insbesondere für die letzte Lehrveranstaltung des Tages.

5. Besondere Richtlinien für Rechner in IT-Räumen

Es gelten alle Richtlinien unter Punkt 2. Die Mitnahme von Speisen und Getränke in die IT-Räume ist untersagt und die Vortragenden sowie die Schüler bzw. Studenten sind dazu angehalten, Räume und Ausstattung sauber zu halten. Die IT-Schulungsräume sind außerhalb der Unterrichtszeiten versperrt; der jeweilige Vortragende muss vor dem Unterricht den Schlüssel für den entsprechenden IT-Raum bei der Information abholen, nach dem Unterricht den Raum wieder versperren und den Schlüssel retournieren. Die Schlüsselausgabe erfolgt ausschließlich für im Infosys gebuchte Schulungen.

Sollte spezielle Software für den Unterricht benötigt werden, so ist dies spätestens 14 Tage vor Unterrichtsbeginn der TCC-IT-Abteilung zu melden; diese wird, sofern technisch möglich, in Zusammenarbeit mit dem Vortragenden eine automatische Installation des betreffenden Software-Pakets via ZenWorks™ erstellen. Lizenzrechtliche Fragen in diesem Zusammenhang sind vom jeweiligen Vortragenden zu klären. Die Rechner der IT-Räume werden ohne Vorankündigung periodisch neu installiert und sind deswegen als Datenablage nicht geeignet.

6. Besondere Richtlinien für die öffentlichen Rechner in der Bibliothek

Es gelten alle Richtlinien unter Punkt 2. Den Schülern und Studenten stehen außerhalb des Unterrichts die Rechner in der Bibliothek zur Verfügung. Private Nutzung in eingeschränktem Maße ist erlaubt, jedoch ist schulischen Recherchen Vorrang einzuräumen. Der Drucker/Kopierer in der Bibliothek kann gegen einen Betrag von

- EUR 0,04/Blatt Schwarz-Weiß
- EUR 0,10/Blatt Farbe

(zahlbar mit Quick) genutzt werden. Die Druckfunktion kann von allen Bibliotheksrechnern aus angesprochen werden.

7. Besondere Richtlinien für spezifische IT-Dienste des TCC

Für alle Dienste gilt: Nutzer können jederzeit von den angebotenen Diensten ausgeschlossen werden, sollte Missbrauch vorliegen oder durch Nutzeraktivität die Systemintegrität gefährdet sein bzw. kurzfristige Eingriffe notwendig sein. Das TCC haftet nicht für Schäden, die ein Nutzer verursacht sowie für Schäden, die einem Nutzer durch den Ausschluss von bestimmten Diensten oder Ausfälle bzw. auftretenden Fehler in der IT-Infrastruktur erwachsen.

7.1 Drahtlose Netzwerke

Den Mitarbeitern der im EWZ angesiedelten Organisationen steht ein eigenes WLAN zur Verfügung. Eine Verbindung kann erst nach der Freischaltung der jeweiligen Hardware-Adresse hergestellt werden. Für Schüler und Studierende sowie Besucher wurde das WLAN „Public“ eingerichtet, welches ohne besondere Vorkehrungen genutzt werden kann, jedoch ohne Unterstützung und Gewährleistung seitens der TCC-IT-Abteilung. Im WLAN „Public“ stehen dem Nutzer die Dienste http und https, VPN, die Maildienste des TCC-Mailsystems, sowie Verbindungen ins UMIT-Forschungsnetz und die Möglichkeit, zur Verfügung. Technische Details sind den jeweiligen Anleitungen auf http://it-portal.t-c-c.at zu entnehmen. Die drahtlosen Netze im EWZ können, falls technisch nötig, jederzeit und ohne Angabe von Gründen von der TCC-IT-Abteilung abgeschaltet werden.

7.2 File- und Printservices

Den Mitarbeitern der im EWZ angesiedelten Organisationen steht Speicherplatz auf Fileservern und verschiedenen Netzwerkdiensten zu Verfügung, und zwar sowohl ein persönlicher „Home“-Bereich als auch je nach Berechtigung verschiedene gemeinsame Laufwerke mit anderen Benutzern. Sowohl der persönliche Speicherbereich als auch ggf. gemeinsame Laufwerke sind über den Novell™-Netware™-Client oder den CIFS-Dienst (Windows-Netzwerk-Emulation) zugänglich. Technische Details sind den Anleitungen auf http://it-portal.t-c-c.at zu entnehmen. Mit Ablage der Daten in einen den Datensicherungsmechanismen unterliegenden Bereich stimmt der Nutzer der Sicherung seiner Daten zu, ebenso einem dadurch entstehenden eventuellen Weiterbestand der Daten nach einer Löschung. Die Letztverantwortung für seinen Datenbestand übernimmt der Nutzer - das TCC haftet nicht für Schäden, die durch technisch bedingte Datenverluste entstehen.

Zugriff auf die Printservices im TCC-Netz erhält der Nutzer über einen entsprechenden Serviceagent und mittels Anmeldung am TCC-Benutzerverzeichnis.

7.3 Webzugang

Die TCC-IT-Abteilung stellt den Zugang zum WWW über einen Proxy zur Verfügung. Dies dient einerseits dem sparsamen Umgang mit Netzwerk-Bandbreite, andererseits der Sperre nicht erlaubter Webseiten. Generell ist der Webzugang ausschließlich zu dienstlichen bzw. studienbezogenen und wissenschaftlichen Zwecken gestattet. Private Nutzung in eingeschränktem Maße wird bis auf Widerruf geduldet, jedoch hat es der Nutzer in jedem Fall zu unterlassen, Seiten folgender Kategorien aufzurufen:

- Seiten mit widerrechtlichen, gewaltverherrlichenden oder pornographischen Inhalten
- Seiten, die urheberrechtlich geschütztes Material zum Download anbieten
- Seiten, die Anleitungen oder Software zur Umgehung von Schutzmechanismen (Cracks, Hacking-Tools,…) oder für kriminellen Handlungen anbieten
- sowie Websites, die als Proxy fungieren

Die TCC-IT-Abteilung ist berechtigt, jederzeit und ohne Angabe von Gründen Websites zu sperren bzw. den Webzugang in Teilen oder insgesamt abzuschalten, soweit dies der Ressourcenplanung, Administration oder der Gewährleistung eines ordnungsgemäßen Systembetriebs dient. Die Nutzung des Webzugangs wird von der TCC-IT-Abteilung protokolliert. Im Falle des Verdachts rechtswidriger oder missbräuchlicher Verwendung werden die protokollierten Daten ausgewertet und bei behördlichen Anfragen weitergeleitet. Ebenso kann in die Zugangsprotokolle Einsicht genommen werden, wenn es zur Beseitigung von Störungen dient. Für erzeugte und versendete Daten beispielsweise in Internet-Foren haftet der jeweilige Nutzer. Das TCC stellt lediglich die Verbindung zum WWW her und ist daher nicht für die Richtigkeit und/oder Vollständigkeit jeglicher übertragener Daten verantwortlich. Ebenso kann der unberechtigte Zugriff Dritter auf vertrauliche Daten nicht vom TCC gewährleistet werden.

7.4 Mailsystem

Das TCC stellt den Nutzern einen Mailaccount in einem Novell™ Groupwise™ Mailsystem zu Verfügung. Der Zugriff auf dieses Mailsystem kann mit dem Groupwise™ Client bzw. dem Webmail-Client erfolgen oder über die Protokolle IMAP und POP3, allerdings wird von der TCC-IT-Abteilung nur der Zugriff über die Groupwise™- und Webmail-Clients unterstützt. Darüberhinaus haben UMIT-Mitarbeiter die Möglichkeit kompatible Smartphones über den Novell DataSynchronizer mit ihrem Groupwise Mailaccount zu synchronisieren. Technische Details sind den Anleitungen auf http://it-portal.t-c-c.at zu entnehmen. Das TCC ist nicht für den Inhalt von versendeten oder empfangenen Nachrichten verantwortlich, sondern allein der jeweilige Absender. Der unberechtigte Zugriff Dritter auf vertrauliche Daten kann nicht ausgeschlossen werden – entsprechende Maßnahmen (z. B. Verschlüsselung) sind vom Nutzer selbst vorzunehmen. Das Versenden von Massen-Mails („Spam“) sowie Mails mit rechts- oder sittenwidrigen Inhalten ist untersagt – entsprechende Beschwerden führen zur Sperre des betreffenden Mailaccounts.

7.5 Sonstige Dienste

Informationen zu den aktuell angebotenen IT-Diensten (Novell Vibe, …) finden Sie auf http://it-portal.t-c-c.at

8. Benutzer-Account

Mitarbeitern und Studierenden wird mit Eintritt ein Benutzer-Account für File- und Mailzugriff eingerichtet. Das zugehörige Initial-Passwort ist unmittelbar nach Erhalt der Benutzerkennung zu ändern. Außerdem werden vom System eine periodische Passwort-Änderung sowie einige Mindestanforderungen zur Beschaffenheit des Passwortes verlangt. Technische Details dazu sind den Anleitungen auf http://it-portal.t-c-c.at zu entnehmen. Der Nutzer ist für die Sicherheit seines Passwortes verantwortlich – für Schäden, die durch kompromittierte Konten entstehen, haftet der jeweilige Inhaber. Die Weitergabe von Zugriffsberechtigungen ist untersagt, es sei denn, es liegt die schriftliche Zustimmung der TCC-IT-Abteilung vor.

9. Definition missbräuchlicher Verwendung

Unter missbräuchlicher Verwendung sind insbesondere jene Handlungen zu verstehen, die u. a. dazu dienen

- den Systembetrieb, bestimmte bzw. sämtliche IT-Dienste oder die Arbeitsstationen anderer Nutzer zu beeinträchtigen oder lahmzulegen (bspw. DOS-Attacken)
- unberechtigten Zugriff auf Computersysteme zu nehmen oder sich unberechtigt Ressourcen (u. a. Passwörter) anzueignen (u. a. Portscans, Sniffer,…)
- Viren oder Würmer in Computernetze einzuschleusen
- sitten- oder rechtswidrige Informationen/Inhalte zu verbreiten bzw. zu beziehen
- urheberrechtlich geschütztes Material anzubieten oder zu beziehen (u. a. über Tauschbörsen)
- Daten im Netzwerk zu manipulieren oder auszuspionieren (bspw. IP-Spoofing oder Manipulation von Mailheadern)
- elektronische Kettenbriefe oder Massensendungen in Umlauf zu bringen
- sich unberechtigt schützenswerte Informationen zu beschaffen und/oder weiterzugeben

10. UMIT-Forschungsnetz

Das TCC betreibt ein vom UMIT-Verwaltungsnetz getrenntes Forschungsnetz. Mitarbeiter der UMIT, die dies wünschen, können ihr System an dieses Forschungsnetz anschließen lassen. Dabei ist folgendes zu beachten:

- Es gelten alle Richtlinien aus Punkt 2.
- Die MAC-Adresse des betreffenden Gerätes muss freigeschaltet und die jeweilige Netzwerkdose umgepatcht werden. MAC-Adresse sowie Dosennummer sind an helpdesk@t-c-c.at zu melden.
- Das TCC betreibt ausschließlich Gateway- und DHCP-Dienste im Forschungsnetz; Dienste des Verwaltungsnetzes können im Forschungsnetz nicht bzw. nur sehr eingeschränkt genutzt werden.
- Das Gerät erhält vom DHCP-Server eine fixe, international gültige IP-Adresse, die nur geringfügigen Firewall-Filtern unterliegt. D.h. der Nutzer muss selbst auf die nötigen Sicherheitsvorkehrungen achten (Virenschutz, Personal-Firewall,...). Die TCC-IT-Abteilung haftet nicht für Schäden am Betriebssystem, Datenverlust o.ä.
- Für Rechner, die an das Forschungsnetz angeschlossen sind, bietet die TCC-IT-Abteilung keinerlei Support
- Es ist nicht gestattet, ein Gerät an beiden Netzen (Verwaltungsnetz und Forschungsnetz) gleichzeitig (beispielsweise über ein 2. Netzwerk-Interface) anzuschließen.
- Missbräuchliche Verwendung (siehe Punkt 9) ist zu unterlassen und zieht dienstrechtliche Konsequenzen nach sich. Im Falle des Verdachts rechtswidriger oder missbräuchlicher Verwendung werden die protokollierten Verbindungsdaten (DHCP-Logs) ausgewertet und bei behördlichen Anfragen weitergeleitet.