INSTITUT FÜR HÖHERE STUDIEN - INSTITUTE FOR ADVANCED STUDIES

BENUTZERInnenORDNUNG

für die Nutzung der

I H S - I T - R e s s o u r c e n

Juli 2020

Nutzungsbeschränkungen

Widmungsgemäß dürfen die IHS-IT-Ressourcen von BenutzerInnen nur im Rahmen wissenschaftlicher, nicht auf Gewinn gerichteter Arbeiten verwendet werden. Das heißt., dass alle Arbeiten, die den Charakter eines direkten persönlichen Vorteils (in Geld oder Geldwert) haben, strikt untersagt sind und rechtliche Folgen haben können. Dasselbe gilt entsprechend für Vorschubleistung an Dritte (z. B. Weitergabe von Login-Kennungen oder Passwörtern). Da das IHS Teilnehmer am österreichischen ACOnet ist, gilt darüber hinaus auch die im Anhang befindliche „**ACOnet Acceptable Use Policy**". Die IHS-IT weist hier insbesondere auf **§3 „Unzulässige Nutzung von ACOnet"** hin.

Software, für die keine entsprechende Nutzungslizenz vorhanden ist, darf weder installiert noch benutzt werden. Bezüglich Software und Softwareversionen, die nicht im IHS-Installationsmenü angeboten werden, insbesondere aber IHS-fremder Software (auch Public Domain Software aus dem Internet!) wenden Sie sich bitte an die IT-Hotline (s.u.).

Login-Kennung, Passwort

MitarbeiterInnen und Gäste des IHS wenden sich um Zuweisung einer Login-Kennung an ihr Sekretariat.

BenutzerInnen haben einen Antrag um Zuweisung der persönlichen Nutzungsberechtigung auszufüllen und zu unterschreiben; man bestätigt damit, diese Benutzerordnung zur Kenntnis genommen zu haben und ihre Bedingungen zu akzeptieren. Mit der Vergabe der Login-Kennung werden ein Passwort und die E-Mail-Adresse(n) mitgeteilt.

Das Passwort darf keinesfalls, in welcher Art auch immer, Dritten (auch nicht der IHS-IT) mitgeteilt werden. BenutzerInnen sind für die Geheimhaltung im Sinne der Datensicherheitsmaßnahmen gemäß DSGVO verantwortlich. Verstöße können rechtliche Konsequenzen nach sich ziehen.

Generelle Verhaltensregeln

- Login-Kennungen und Passwörter sind strikt geheimzuhalten. IHS-Passwörter dürfen nicht unverändert auch für externe Dienste (Online Shops, Mail-Dienste etc.) eingesetzt werden.
- IT-Equipment ist schonend zu behandeln (Ess-, Trink- und Rauchverbot wegen Tastaturproblemen u.ä.).
- An die grün (manchmal auch rot!) gekennzeichneten Steckdosen darf nur IT-Equipment angeschlossen werden.
- Geräte- und Netzwerkverkabelungen dürfen nicht geöffnet werden. Dazu sind nur IT-Personal bzw. WartungstechnikerInnen berechtigt.
- Einrichtung und Betrieb von zusätzlichen Kommunikationsdiensten (Modems, Serverdienste, WLAN-Access Points usw.) sind untersagt, jegliche Maßnahmen zur Umgehung bzw. Störung des Netzwerk- und Security-Setups sind verboten.
- Eingriffe in PC-Konfigurationen dürfen nur durch IT-Personal vorgenommen werden.
- Ein Standortwechsel der Geräte darf nur durch IT-Personal vorgenommen werden.
- Bei physischer Abwesenheit vom Gerät ist dieses durch Aktivieren der Bildschirmsperre zu sichern. Bei öffentlich zugänglichen Geräten hat nach der Beendigung der Arbeit ein Logout oder Shutdown zu erfolgen.
- Wichtige Dateien der BenutzerInnen sind auf jeden Fall auch auf den Netzplatten H:\ und J:\ bzw. „Documents" abzulegen, da sie sonst im Falle eines Crashs der lokalen Platte nicht wiederherzustellen sind. Nur von Dateien auf H:\ und J:\ wird täglich eine Sicherungskopie (Backup) erzeugt. Ebenso sind nur von Dateien auf H:\ und J:\ sämtliche Änderungen während des letzten Monats auf dem Netzlaufwerk K:\ wieder abrufbar.
- **Hinweis**: bei Auslagerung von Dateien zu externen Speicherdiensten (z. B. Dropbox, SugarSync etc.) kann die IHS-IT keinerlei Haftung für Verfügbarkeit, Datenverlust usw. übernehmen. Aus Datenschutzgründen wird von der Verwendung solcher Dienste, insbesondere für unternehmensrelevante Daten, abgeraten. Handelt es sich um personenbezogene Daten gemäß DSGVO, ist eine Speicherung dieser in der Regel unzulässig.

- Für die Sicherung der Dateien auf lokalen Platten wie D:\ sind die BenutzerInnen persönlich verantwortlich.
- Sollen lange Programm-Jobs über eine oder mehrere Nächte laufen, so ist vorher die IT-Hotline zu kontaktieren.
- Ein persönlich zugeordneter PC darf von Dritten nur nach Absprache mit der Geräteinhaberin bzw. dem Geräteinhaber benützt werden, ausgenommen, es handelt sich um Wartungsarbeiten durch die IHS-IT.
- Bei Störungen an einem Gerät ist sofort die IT-Hotline zu verständigen.
- Es ist verboten, Software, Hardware oder Betriebsmittel (Papier!) sowie Dokumentationen an Dritte weiterzugeben.
- Automatische Virentests dürfen weder umgangen noch unterbrochen werden.
- Nicht im IHS beschriebene Speichermedien (z. B. CD-ROMs, USB-Memory Sticks …) dürfen nur nach vorherigem Viren-Check verwendet werden. Diese Checks sind von den BenutzerInnen selbst **vor** der Verwendung durchzuführen. Sollte der Test anzeigen, dass das Medium Viren enthält, die nicht erfolgreich entfernt werden konnten, ist sofort die IT-Hotline zu verständigen.

Zusätzliche Verhaltensregeln für die Benutzung von öffentlichen PCs bzw. Netzdruckern

- An öffentlichen PC-Arbeitsplätzen herrscht striktes Ess-, Trink- und Rauchverbot.
- Es dürfen keine Gegenstände (Geräte, Geräteteile, Handbücher, Sessel etc.) von den Standorten öffentlicher PC-Arbeitsplätze, oder von Clean-Desk-Arbeitsplätzen, entfernt werden.
- Persönliche Dateien der BenutzerInnen sind, wenn auf lokalen Platten nötig, in Unterverzeichnissen von D:\Data\USER abzulegen, besser aber auf der Netzplatte H:\. Benutzerdateien, die in anderen Verzeichnissen gespeichert sind, können bei den regelmäßigen, mindestens aber einmal pro Jahr stattfindenden, PC-Standard-Setups ohne Vorwarnung gelöscht werden.
- Nach Beendigung der Arbeit ist der PC-Arbeitsplatz aufgeräumt zu hinterlassen. Papier, das nicht mehr benötigt wird, ist in den dafür vorgesehenen Altpapier-Schachteln zu deponieren.
- Netzdrucker dürfen weder abgeschaltet noch umkonfiguriert werden.

Betriebsmittelausgabe

- Papier für die Drucker wird von IHS-IT-Personal bereitgestellt und von BenutzerInnen bei Bedarf nachgefüllt.
- Toner wird im Regelfall von IHS-IT-Personal gewechselt.

Aktuelle Informationen

Betriebszeiten:		Mo - So, 00:00 - 24:00 Uhr
IT-Hotline:	++43 1 59991-**222** hotline@ihs.ac.at	Mo - Fr, 08:30 - 18:30 Uhr

Weitere Informationen (z. B. über IT-Hotline, Passwortänderung, Softwareinstallation, Webmail) finden Sie in den Web-Seiten unter https://ihs.ac.at/it.

Wartungsarbeiten
Wartungsarbeiten können zu teilweisen oder vollständigen Stillständen der angebotenen Dienste führen. Über diese Wartungsarbeiten wird, soweit diese geplant sind, im Voraus per E-Mail informiert. BenutzerInnen haben in solchen Fällen selbst dafür Sorge zu tragen ihre Arbeit rechtzeitig zu unterbrechen, offene Dateien zu speichern und zu schließen bzw. ein Logout durchzuführen, unabhängig davon, ob sie vor Ort arbeiten oder IHS Dienste mittels Remote Access nutzen.

Sonstige Richtlinien, Änderungsvorbehalt
Diese Richtlinie ist in ihrer jeweils aktuellen Fassung auf der Website https://www.ihs.ac.at/it im Abschnitt „Users and Visitors“ abrufbar. Andere Teilbereiche oder Dienste (Beispielsweise E-Mail-Filterung) sind in getrennten Richtlinien geregelt, diese finden sich ebenfalls im o. g. Abschnitt. Über Änderungen dieser Richtlinien oder die Neuregelung eines Teilbereiches informiert die IHS-IT alle BenutzerInnen per Mail an ihre IHS-E-Mail Adresse.

Die Durchführung bestimmter Projekte kann, z. B. auf Verlangen von AuftraggeberInnen, die Einhaltung besonderer Sicherheitsmaßnahmen erfordern. In einem solchen Fall können die mit dem Projekt befassten Personen von der Geschäftsführung zur Einhaltung besonderer Sicherheitsmaßnahmen verpflichtet werden.

Anhang

ACOnet Acceptable Use Policy (ACOnet-AUP)

Allgemeine Benutzungsordnung für die Services von ACOnet

§ 1 Zweck von ACOnet

Das österreichische akademische Computernetz ACOnet dient den gemeinnützigen Institutionen der Forschung, Bildung und Kultur Österreich. Die Grundsätze für die Teilnahme an ACOnet, insbesondere die von ACOnet erbrachten Leistungen und Services, sind unter http://www.aco.net/aconet-teilnahme.pdf veröffentlicht.

§ 2 Teilnahme an ACOnet

ACOnet erbringt ein Internet-Backbone-Service, jede an ACOnet teilnehmende Einrichtung ist für den Betrieb ihres lokalen Netzwerkes und die Bereitstellung der individuellen Netzdienste für ihre eigenen Benutzer selbst verantwortlich. Insbesondere trägt jede teilnehmende Einrichtung die Verantwortung für die Einhaltung der ACOnet-AUP durch die individuellen Benutzer aus ihrem eigenen Bereich und erläßt hierfür eine entsprechende lokale Benutzungsordnung. Jede teilnehmende Einrichtung betraut eine geeignete Person aus ihrem Bereich mit der Funktion des lokalen Sicherheitsbeauftragten, der die Einhaltung der ACOnet-AUP gewährleistet.

§ 3 Unzulässige Nutzung von ACOnet

Die Services von ACOnet werden für die teilnehmenden Institutionen zur Erfüllung ihrer eigenen Aufgaben erbracht, eine Inanspruchnahme für gewerbliche Zwecke sowie eine Weitergabe an fremde Einrichtungen ist grundsätzlich nicht zulässig, allfällige Ausnahmen bedürfen einer Regelung gemäß § 1 Abs. 7 und 8 der „Grundsätze für die Teilname an ACOnet“.

Unzulässig ist ferner die bewußte Inanspruchnahme von ACOnet-Diensten zur Übertragung, Verbreitung oder Speicherung von Daten, welche

- gegen bestehende Gesetze verstößt oder die öffentliche Ordnung oder die Sittlichkeit gefährdet,
- Schutzrechte anderer (z.B. Datenschutz, Urheberrecht) verletzt,
- andere Netzteilnehmer behindert, belästigt oder verängstigt (z.B. Spam),
- schädliche Komponenten (z.B. Viren, Trojanische Pferde) enthält,
- zur Erlangung eines unautorisierten Zugriffs dient (z.B. Portscan, Passwort-Scan, Ausnützung von Systemschwächen),
- eine Beeinträchtigung des Netzbetriebs beabsichtigt (z.B. bewußtes Herbeiführen eines Systemabsturzes, DoS Attacken).

§ 4 Maßnahmen bei Verstößen

Die an ACOnet teilnehmenden Einrichtungen sind angehalten, bei Verstößen gegen die ACOnet-AUP den Mißbrauch unverzüglich abzustellen sowie im erforderlichen Ausmaß den ACOnet-Betreiber zu informieren. Sollte es zur Aufrechterhaltung oder Wiederherstellung eines geordneten Betriebs der ACOnet-Services erforderlich sein, einzelne Personen oder Einrichtungen von der Nutzung der angebotenen Dienste oder von Teilen derselben auszuschließen, so ist der ACOnet-Betreiber berechtigt, entsprechende Maßnahmen zu setzen und gleichzeitig darüber den zuständigen lokalen Sicherheitsbeauftragten zu informieren. In besonders schwerwiegenden Fällen, bei denen die unzulässige Nutzung eine Verletzung von geltendem Recht darstellt, können zivil-oder strafrechtliche Schritte eingeleitet werden.

§ 5 Schlussbestimmungen

Änderungen der ACOnet-AUP sind vorbehalten, bedürfen jedoch des Beschlusses des ACONET-Vereinsvorstandes. Die jeweils gültige Fassung der ACOnet-AUP ist unter http://www.aco.net/aconet-aup.pdf veröffentlicht. Meldungen über Verstöße gegen die ACOnet-AUP sind an <abuse@aco.net> zu richten.