Kanton St.Gallen
Bildungsdepartement

Cluster I – BWZ Rapperswil-Jona

Informatik Leitfaden für Lehrpersonen, Lernende und Kursteilnehmer

Kanton St.Gallen
Bildungsdepartement

Cluster I – BWZ Rapperswil-Jona

1 Persönlicher Account (Zugangsdaten)

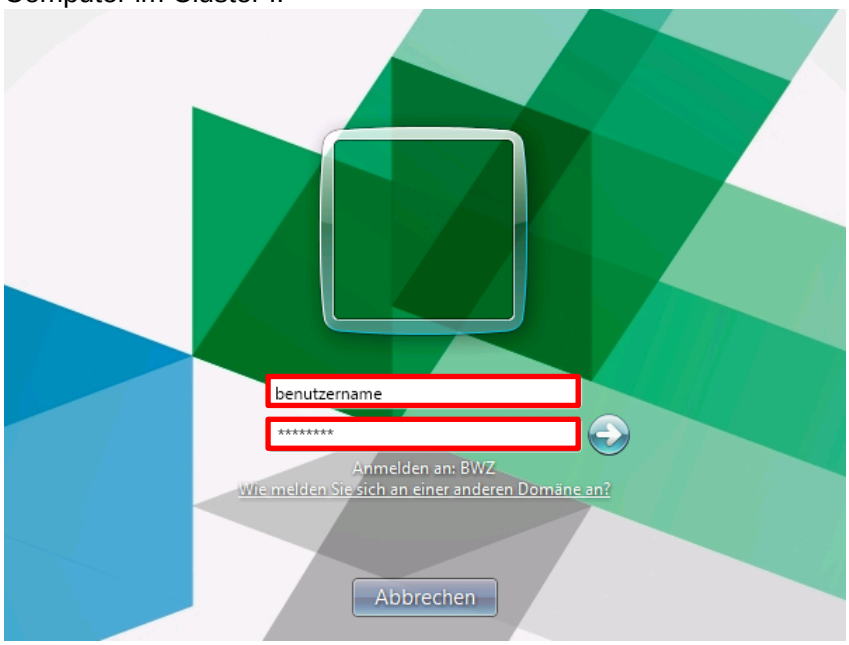
Mit dem Start des Unterrichts/Lehrgangs im Cluster I erhalten Sie von IT Services einen persönlichen Account (Zugangsdaten) bestehend aus

Benutzername	*vorname.nachname*
Kennwort	*[Ihr persönliches Kennwort erhalten Sie von Ihrer Klassenlehrperson]*
E-Mail*	*vorname.nachname@bwz-rappi.ch*

*bei Kursteilnehmern wird automatisch eine Weiterleitung an die private E-Mailadresse eingerichtet

2 Anmeldung an einem Computer im Cluster I

Verwenden Sie Benutzername und Kennwort Ihres persönlichen Accounts für die Anmeldung an einem Computer im Cluster I.



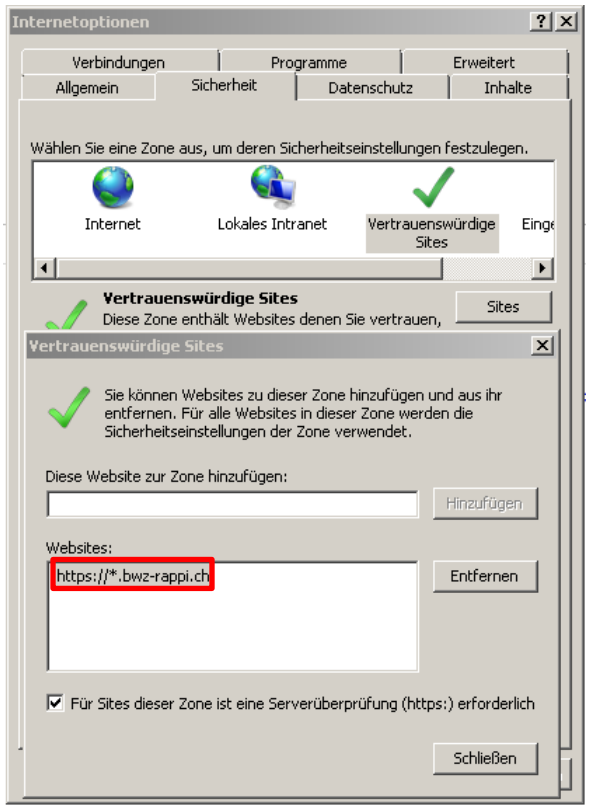
3 Anmeldung an UAG (externer Zugang)

Sie haben weltweiten Zugang – über UAG – auf diverse Dienste (Portal, Outlook Web App, …) des Cluster I.

Die URL für den externen Zugang lautet *https://iag.bwz-rappi.ch*

Verwenden Sie Benutzername und Kennwort Ihres persönlichen Accounts für die Anmeldung an UAG.

Um Probleme beim Zugriff auf den UAG zu verhindern, muss die Website *https://*.bwz-rappi.ch* unter *Vertrauenswürdige Sites* hinzugefügt werden.
Internet Explorer – Extras – Internetoptionen – Sicherheit – Vertrauenswürdige Sites – Sites – https://.bwz-rappi.ch/* hinzufügen

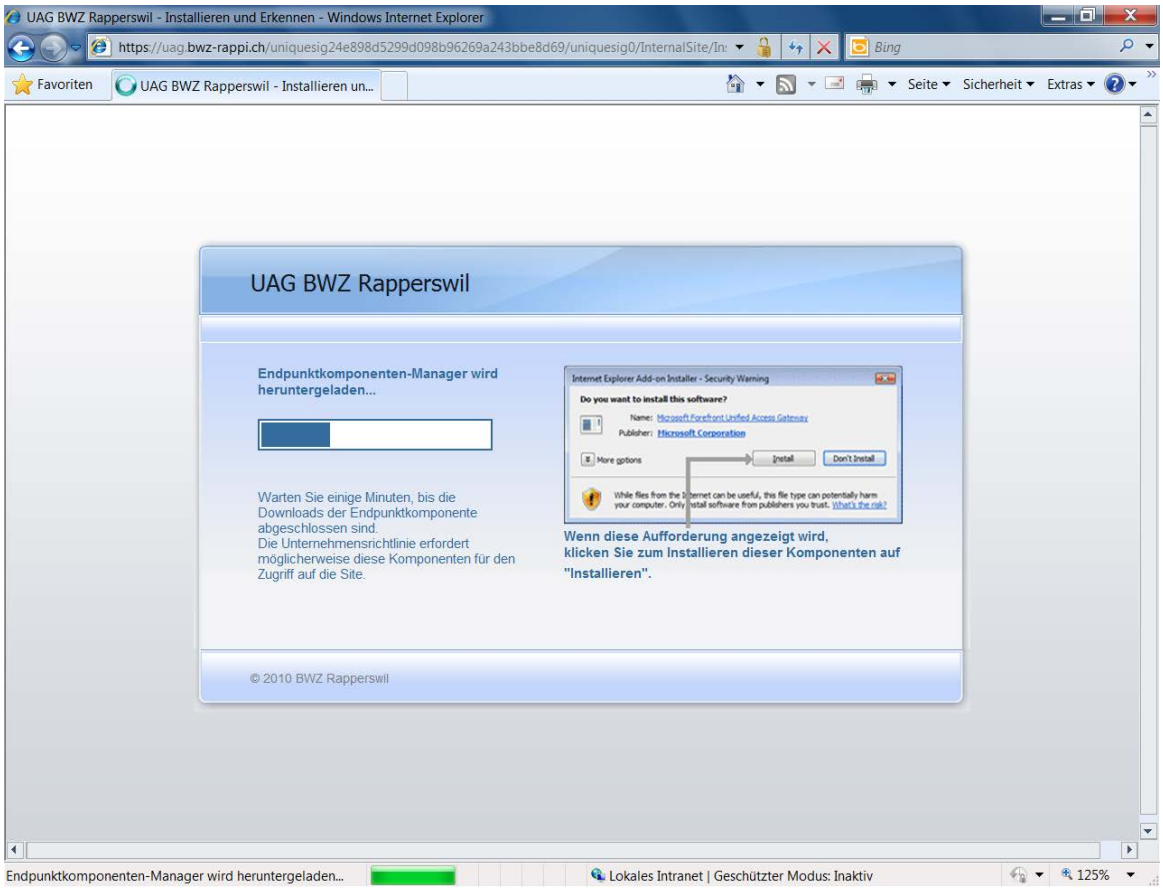


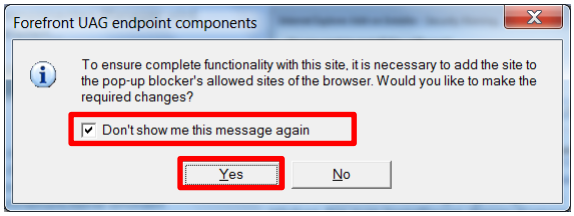
Kanton St.Gallen
Bildungsdepartement

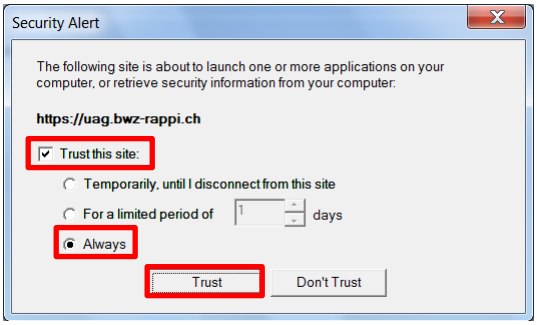
Cluster I – BWZ Rapperswil-Jona

Zur Nutzung sämtlicher Funktionen von UAG empfehlen wir die Verwendung von Microsoft Windows 7 und Internet Explorer 9. Der Zugriff mit anderen Betriebssystemen und Browsern ist möglich, es muss aber mit Einschränkungen gerechnet werden.

Beim ersten Zugriff auf den UAG müssen einmalig folgende Einstellungen vorgenommen werden:







4 Kennwort

Bitte ändern Sie nach Erhalt ihres persönlichen Accounts Ihr Kennwort. Aus Sicherheitsgründen müssen bei der Kennwortänderung folgende Regeln eingehalten werden:

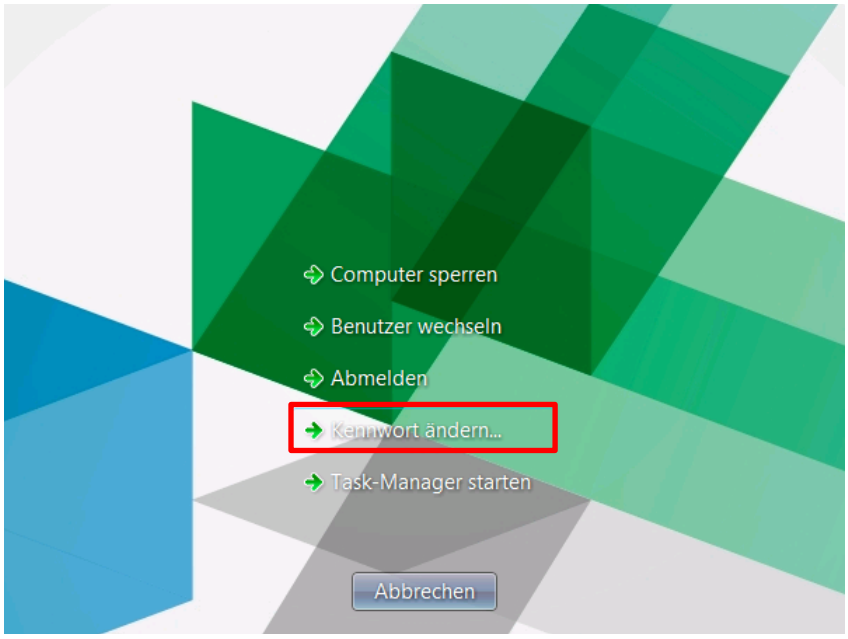
- Das Kennwort muss mindestens 7 Zeichen lang sein
- Das Kennwort muss folgende drei Kriterien erfüllen:
  Grossbuchstaben (A-Z)
  Kleinbuchstaben (a-z)
  Zahlen (0-9) oder Sonderzeichen (!, ?, @, %, &, …)
- Das Kennwort darf keine Namen oder Teile aus dem Benutzernamen enthalten

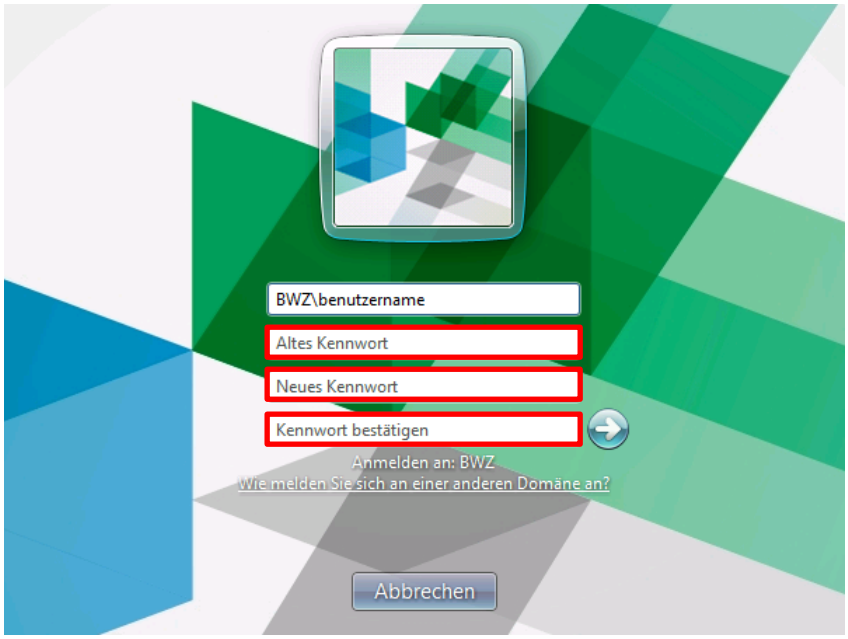
Weiter ist folgendes zu beachten:

- Ihr persönlicher Account wird nach 5 Fehleingaben für 5 min gesperrt.
- Ihr Kennwort läuft nach 120 Tagen ab und muss geändert werden.
- Das gleiche Kennwort kann frühestens nach 21 Kennwortänderungen wieder verwendet werden.

4.1 Kennwort ändern an einem Computer im Cluster I

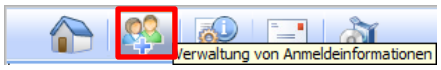
Melden Sie sich an einem Computer im Cluster I an (gemäss Punkt 2). Drücken Sie nach erfolgreicher Anmeldung *ALT + CTRL + DEL* und wählen Sie *Kennwort ändern* und füllen Sie danach die Felder entsprechend aus.





4.2 Kennwort ändern an UAG (externer Zugang)

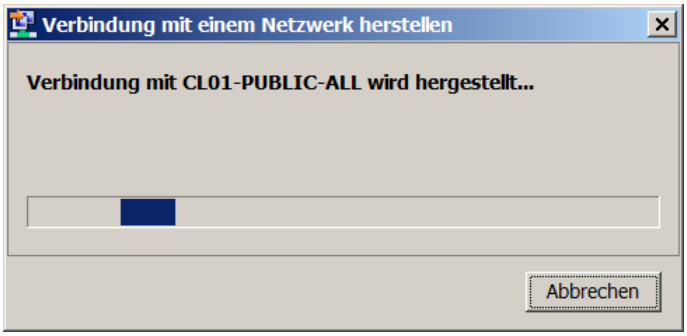
Melden Sie sich an UAG an (gemäss Punkt 3). Klicken Sie nach erfolgreicher Anmeldung auf das Symbol *Verwaltung von Anmeldeinformationen*, wählen Sie *Kennwort ändern* und füllen Sie danach die Felder entsprechend aus.



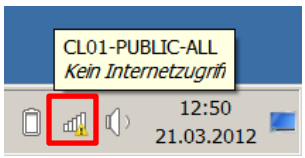
5 WLAN

5.1 WLAN-Zugang mit Notebooks (Windows, via Landing-Page)

Wählen Sie das Netzwerk *CL01-PUBLIC-ALL.*



Nach erfolgreicher Herstellung der Verbindung wird nachfolgendes Symbol in der Taskleiste ersichtlich.



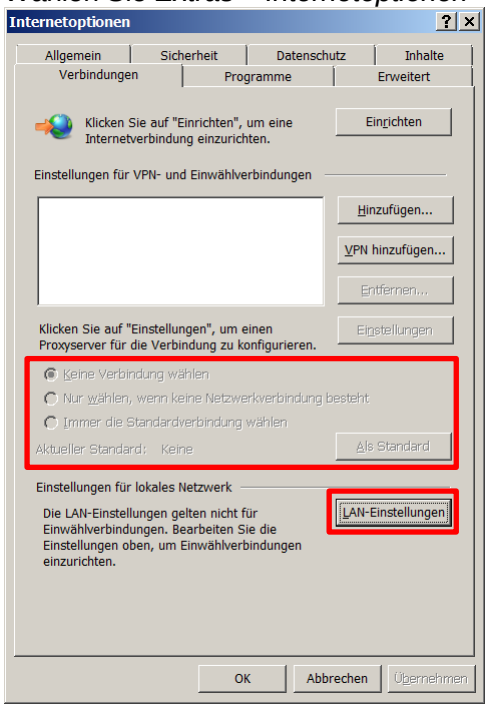
Beim Öffnen des Browsers werden Sie automatisch auf die Landing-Page weitergeleitet. Verwenden Sie Benutzername und Kennwort Ihres persönlichen Accounts für die Anmeldung am WLAN.

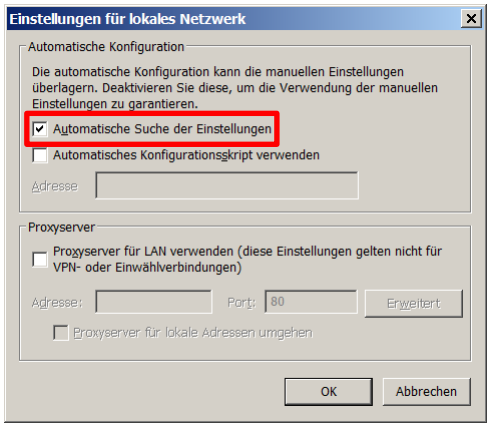
Kanton St.Gallen
Bildungsdepartement

Cluster I – BWZ Rapperswil-Jona

Problembehandlung

Sollte trotz erfolgreicher Anmeldung der Zugriff auf das Internet nicht möglich sein, überprüfen Sie die Einstellungen in ihrem Browser (z.B. Internet Explorer 9).
Wählen Sie *Extras – Internetoptionen – LAN-Einstellungen* und nehmen Sie folgende Einstellungen vor.





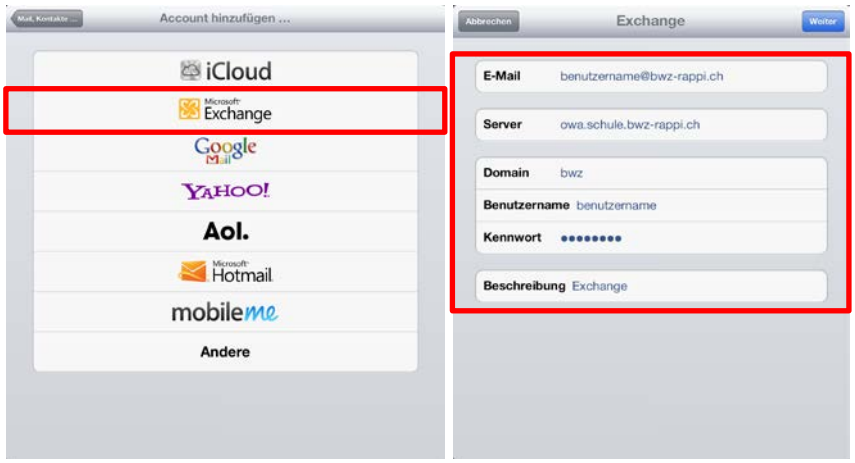
5.2 WLAN-Zugang mit Smartphones (iOS, via EAP)

Wählen Sie das Netzwerk *CL01-PUBLIC-EAP.*

Verwenden Sie Benutzername und Kennwort Ihres persönlichen Accounts für die Anmeldung am WLAN.

6 Exchange-Konto auf Smartphones/Tablets (iOS)

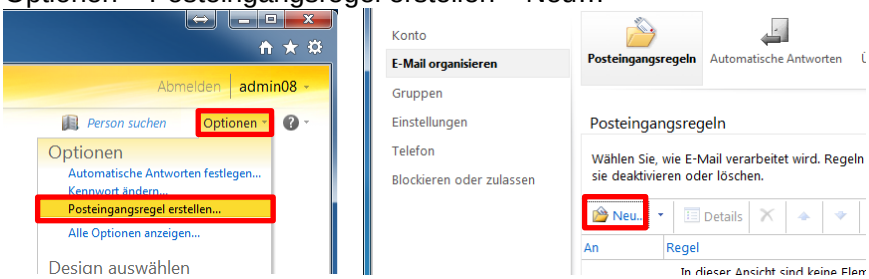
Sie können Ihr persönliches Exchange-Konto (E-Mail, Kalender, Kontakte) mit Ihrem privaten Smartphone oder Tablet synchronisieren. Wählen Sie Microsoft Exchange und verwenden Sie Benutzername und Kennwort Ihres persönlichen Accounts.



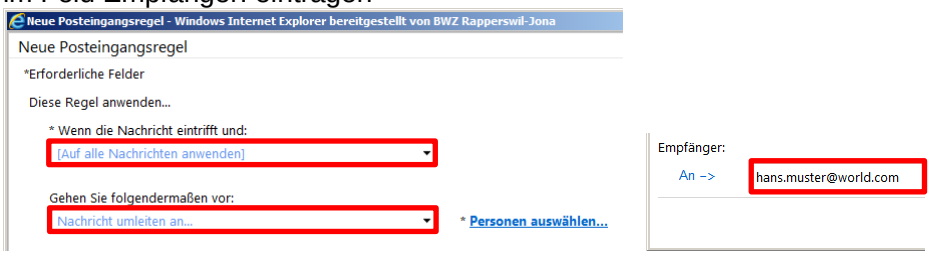
7 Exchange-Konto Weiterleitung

Sie können Ihr persönliches Exchange-Konto resp. Ihre persönliche E-Mail-Adresse auf eine andere E-Mail-Adresse weiterleiten. Melden Sie sich von Extern an UAG an und gehen Sie wie folgt vor:

- Outlook Web App
- Optionen – Posteingangsregel erstellen – Neu…



- [Auf alle Nachrichten anwenden], Nachrichten umleiten an..., E-Mail-Adresse für Weiterleitung im Feld Empfänger: eintragen



8 Wartungsfenster

Montag von 22:00 Uhr bis Dienstag 06:00 Uhr. Während eines Wartungsfensters ist die Anmeldung an einem Computer im Cluster I sowie die externe Anmeldung an UAG grundsätzlich nicht möglich

9 Nutzungsvereinbarung

9.1 Gültigkeit

- Diese Benutzungsordnung gilt für alle Angehörigen des Cluster I sowie für Dritte. Unter Dritte sind alle Nutzer und Nutzerinnen zu verstehen, die Informatikmittel im Cluster I nutzen und/oder ein Benutzerkonto besitzen.
- Unter dem Begriff Anwendung oder Verwendung ist jede Art von elektronischer Bearbeitung von Daten mittels Geräten, Programmen oder Diensten zu verstehen.
- Als Angehörige des Cluster I gelten sämtliche Dozierende, Lernende und übrige Mitarbeiterinnen und Mitarbeiter des Cluster I.

9.2 Benutzung der Informatikzimmer und der Informatikmittel

- In den Informatikzimmern installierte Geräte und aufliegende Unterlagen dürfen nicht aus diesen Räumen entfernt werden.
- Es gelten zusätzlich die bei den Informatikzimmern angeschlagenen Vorschriften.
- Grundsätzlich dürfen keine Änderungen an den Geräten vorgenommen werden (Hardware und Software).
- Jede private, gewerbliche oder entgeltliche Nutzung von Informatikmitteln des Cluster I ist nicht statthaft, wenn dies nicht ausdrücklich genehmigt ist.
- In den Informatikzimmern gelten die allgemeinen Regeln der Cluster I Hausordnung (Rauch-, Ess- und Trinkverbot).

9.3 Schutz von Endgeräten und Kennwort

- Die Computer dürfen in der Abwesenheit von Nutzerinnen und Nutzern nicht unautorisiert bedient werden, der Computer muss deshalb beim Verlassen des Arbeitsplatzes gesperrt oder ausgeschaltet werden.
- Zum Schutz der Programme und Daten teilt IT Services allen Nutzerinnen und Nutzern einen Benutzernamen mit Kennwort zu, mit denen auf Ressourcen im Netzwerk zugegriffen werden kann. Dieses Kennwort ist nach der ersten Anmeldung umgehend zu ändern.
- Das Kennwort ist streng vertraulich und darf nicht weitergegeben werden. Nutzerinnen und Nutzer können verantwortlich gemacht werden, wenn mittels Ihres Kennwortes unberechtigt auf Daten zugegriffen wird.
- Nutzerinnen und Nutzer sind für die Verwaltung Ihres Kennwortes verantwortlich.
- Das Kennwort muss nach den Richtlinien der Kennwortrichtlinie gewählt und regelmässig gewechselt werden.
- Das Ausprobieren, das Ausforschen und die Benutzung fremder Zugriffsberechtigungen (z.B. Log-in, Passwörter, persönliche Identifikationsausweise usw.) und sonstiger Authentifizierungshilfsmittel (z.B. Chipkarten, Magnetkarten, usw.) sind verboten.

9.4 Umgang mit Daten und Programmen

- Jede missbräuchliche Beschaffung von Daten ist verboten.

- Text-, Bild- und Tondokumente, die nicht im Interesse des Cluster I liegen, dürfen nicht im Cluster I verwendet, bearbeitet oder auf den IT-Systemen des Cluster I gespeichert werden.
- Daten, welche nicht auf den zentralen Datenablagesystemen gespeichert sind, werden durch IT Services nicht gesichert. Die Nutzerin oder der Nutzer ist für die Sicherung dieser Daten (z. B. auf der lokalen Festplatte) selber verantwortlich.
- Vertrauliche Daten dürfen nur von befugten Personen eingesehen und bearbeitet werden. Diese sind dafür verantwortlich, dass solche Daten nur auf den vorgesehenen Datenablagen abgelegt und mit den vorgesehenen Zugriffsmitteln (z.B. Computer) eingesehen und bearbeitet werden. Sie sind ebenfalls dafür verantwortlich, dass über ihre Zugriffsmittel unbefugte Personen keinen Zugriff auf vertrauliche Daten erhalten.
- Das Ausführen, Installieren und zur Verfügung stellen von Computerspielen jeglicher Art ist in den Informatikzimmern untersagt. Ebenso sind jegliche Netzwerkspiele über das Netzwerk untersagt.

9.5 Wechseldatenträger

Wechseldatenträger (z.B. USB-Stick, CD, DVD etc.) können grundsätzlich eingesetzt werden. Folgende Rahmenbedingungen müssen jedoch eingehalten werden:

- Die Verantwortung für die gespeicherten Daten liegt vollumfänglich beim Benutzenden.
- Eine Weitergabe von vertraulichen Daten darf nur anonymisiert oder verschlüsselt mit einer entsprechenden Geheimhaltungserklärung erfolgen.
- Wechseldatenträger mit vertraulichen Daten müssen bei der Entsorgung zerstört werden.
- USB-Sticks sollten Kennwortgeschützt und die Daten sollten verschlüsselt sein.

9.6 Nutzung von Internetdiensten

- Die Benutzung der Internetdienste hat im Zusammenhang mit dem Auftrag des Cluster I, d.h. Lehre, Weiterbildung oder Forschung zu stehen.
- Unzulässig ist der Zugriff auf Websites mit:
  - Inhalte, welche einen Straftatbestand nach schweizerischem Strafgesetzbuch (SR 311.0) erfüllen (Bsp. qualifizierte Pornographie nach Artikel 197).
  - rassistischem oder gewaltverherrlichendem Inhalt
  - Inhalten, die sonst wie gegen die gute Sitten verstossen.
- Die Benutzung der Internetdienste für private Zwecke ist untersagt. Für einfache Tätigkeiten, welche den Internetzugang nur minimal beanspruchen, wie z. B. das Einsehen des Fahrplanes der SBB, darf der Internetzugang trotzdem privat genutzt werden.
- Downloads und Uploads für private Zwecke (z.B. MP3, Bilder etc.), das Hören von Musik und das Ansehen von Filmen über Internet sind nicht gestattet.
- Der Einsatz von Software für das Tauschen von Daten wie Musik oder Filme ist untersagt.

9.7 Virenschutz

Das Virenprogramm und die Virensignaturdatei von Computern des Cluster I werden periodisch durch eine neue Version ersetzt, damit auch neue Virentypen erkannt werden können. Die Funktion der automatischen Aktualisierung wird durch IT Services für Computer des Cluster I konfiguriert und regelmässig überprüft. Es ist untersagt, die Virenschutzprogramme auf den Computern des Cluster I abzuschalten.

9.8 Nutzung von Maildiensten

- Die Benutzung der Cluster I Maildienste ist verboten für:
  - Spam Mails
  - Politische Zwecke
  - Private Werbezwecke
  - Mails mit rechtswidrigen Inhalten
- Die Cluster I E-Mail Adressen dürfen nur im Zusammenhang mit dem Auftrag im Cluster I verwendet werden.
- Die private Nutzung der Maildienste ist zurückhaltend auszuüben.
- Das automatische Weiterleiten von E-Mails auf private oder sonstige externe Mailboxen ist untersagt. Für den permanenten Zugriff auf die Cluster I Mailbox, ist UAG zu verwenden.
- Verdächtige Mails sind unbesehen aus dem Posteingang zu löschen. Vorsicht ist insbesondere geboten bei auffälligen Betreff-Angaben, auch wenn die Mails von bekannten Absendern stammen. Vertrauliche Informationen dürfen nicht ungeschützt und unverschlüsselt als E-Mail versandt werden.

9.9 Clear-Desk Regelung

Beim Verlassen des Arbeitsplatzes am Feierabend, ist der Arbeitsplatz ordnungsgemäss aufzuräumen. Dies bedeutet:

- Vertrauliche Dokumente in gedruckter Form sind in den entsprechenden Aktenschränken oder im Pult einzuschliessen.
- Nicht mehr benötigte vertrauliche Dokumente sind zu vernichten (Aktenvernichter) oder in den vorgesehenen Behältnissen zu entsorgen. Sie gehören nicht in den Papierkorb.
- Beim Verlassen des Arbeitsplatzes, auch nur für kurze Zeit, ist der Computer mit einem Kennwortschutz zu sperren.
- Bei längerer Abwesenheit und über Nacht ist der Computer ordnungsgemäss herunterzufahren.
- Die Fenster und Türen sind zu schliessen.
- Die Bürotüre ist, wenn möglich, abzuschliessen.
- Türen zu Nebenräumen mit vertraulichen Daten oder wertvollem Inhalt sind abzuschliessen.

9.10 Verwendung privater Geräte (Notebook, PDA/Organizer, Smartphone)

- Die Nutzung privater Geräte ist im Cluster I Netzwerk grundsätzlich nicht erlaubt.
- Die Nutzung privater Geräte im dafür vorgesehenen WLAN ist erlaubt.
- PDAs/Organizer oder Smartphones sind nur nach Absprache mit IT Services zulässig. Ohne Einwilligung IT Services darf keine entsprechende Synchronisationssoftware installiert werden.

9.11 Urheberecht und Nutzung

- Ohne die schriftliche Zustimmung der Trägerschaft von Autoren- und Lizenzrechten ist es nicht gestattet, Software, Text-, Bild- und Tondokumente zu kopieren oder zu referenzieren.
- Die Rechte an Programmen, Software- Text-, Bild- und Tondokumente, die in Projekten der Institute mit der Industrie entstehen, sind in speziellen Verträgen durch die zuständigen Verantwortlichen zu regeln. Die Verantwortung für die Einhaltung der Lizenzbestimmungen liegt beim Projektleiter.
- Alle sonst durch Angehörige im Cluster I entwickelten Programme, Software, Text- Bild- und Tondokumente sind ohne Lizenzen und Gebühren für Angehörige des Cluster I frei nutzbar.

9.12 Missbrauch, Kontrolle und Sanktionen

Als Missbrauch gilt:

- die Verletzung der vorliegenden Vorschriften
- die Verletzung von übergeordnetem Recht
- unverhältnismässige oder nicht bewilligte Benutzung der Informatikmittel
- Verletzung von Lizenzrechten
- Verletzung des Datenschutzes
- Verletzung des Urheberrechts
- Speichern, Drucken, Versenden oder Darstellen von Daten die mit dem Auftrag und Ansehen des Cluster I unvereinbar sind, insbesondere Daten rassistischen, rechtsradikalen, sexistischen oder pornografischen Inhaltes.
- IT Services überwacht die technischen Ressourcen in Form von automatisierten Protokollierungen (Virenscanner, Speicherauslastung usw.)
- Bei Verdacht auf Missbrauch ist der IT-Sicherheitsbeauftragte, in Absprache mit seinem Vorgesetzten, befugt, Daten zu Beweiszwecken sicherzustellen; betrifft datenschutzrelevante Daten und nur sofern zeitkritische Intervention notwendig. Logfiles sind davon ausgenommen.
- Bei Missbrauch ist der IT-Sicherheitsbeauftragte, in Absprache mit seinem Vorgesetzten befugt, den Zugang zu Informatikmitteln zu sperren oder Daten zu löschen.
- Die Schulleitung des Cluster I entscheidet auf Antrag des IT-Sicherheitsbeauftragten über die Einleitung eines Disziplinar- oder Strafverfahrens.
- Kosten, die dem Cluster I im Zusammenhang mit Missbrauch entstehen, werden dem Verursacher oder der Verursacherin belastet. Bei Urhebermissbrauch lehnt der Cluster I jede Verantwortung und Haftung ab. Der Verursacher bzw. die Verursacherin haftet für die Folgen selber.

9.13 Übergeordnetes Recht

Die vorliegenden Bestimmungen stützen sich vornehmlich auf die Bundesgesetze des Urheberrechts und des Datenschutzes, sowie auf die vertraglichen Vereinbarungen, die der Cluster I oder ihr assoziierte Gruppen über Lizenzen und Dienstleistungen jeder Art abgeschlossen haben. Die massgebenden Rechtsvorschriften sind nebst den Lizenzvereinbarungen, ZGB und OR folgende gesetzliche Bestimmungen:

- DSG Datenschutzgesetz
- FMG Fernmeldegesetz
- PatG Patentgesetz
- URG Urheberrechtsgesetz
- URV Urheberrechtsverordnung

IT Services
helpdesk@bwz-rappi.ch

Rapperswil, 5. September 2012