RAHMENBETRIEBSVEREINBARUNG ÜBER DIE EINFÜHRUNG UND DEN EINSATZ VON INFORMATIONS- UND KOMMUNIKATIONSSYSTEMEN (IuK) AN DER MÜNCHNER VOLKSHOCHSCHULE (MVHS)

1. Ziel der Betriebsvereinbarung

Ziel der Betriebsvereinbarung ist es, die Einführung und Anwendung aller technischen Einrichtungen, die eine Überwachung oder Verhaltens- und Leistungskontrolle der Mitarbeiter/innen ermöglichen könnten, als Anlagen zu dieser Rahmenbetriebsvereinbarung zu regeln. Geschäftsführung (MVHS) und Betriebsrat (BR) stimmen darin überein, dass die Betriebsvereinbarung zum Schutz der einzelnen Arbeitnehmer/innen anlässlich der Einführung der o.g. Systeme geschlossen wird. Außerdem wird ein Mitbeurteilungsrecht des Betriebsrates bei der Ermittlung der Grenze zwischen zulässigen und unzulässigen Eingriffen eingeräumt.

Diese Betriebsvereinbarung regelt die Handhabung gesetzlicher Bestimmungen, insbesondere solcher des BetrVG, an der MVHS.

Die Verantwortung für die Einhaltung der Regeln in dieser Vereinbarung liegt sowohl beim Arbeitgeber, der durch geeignete organisatorische Maßnahmen sicherstellen muss, dass das Vereinbarte eingehalten wird als auch bei den Mitarbeiter/innen selbst. Verstöße gegen die Betriebsvereinbarung und ergänzende Bestimmungen können zum Entzug von Zugriffsrechten, aber auch zu arbeitsrechtlichen und strafrechtlichen Konsequenzen führen. Die gesetzlichen Beteiligungs- bzw. Mitbestimmungsrechte des BR bei arbeitsrechtlichen Verstößen, insbesondere nach dem BetrVG, bleiben hiervon unberührt.

2. Geltungsbereich der Betriebsvereinbarung

Diese Betriebsvereinbarung ist eine Rahmenbetriebsvereinbarung, die sich auf alle Elemente von Informations- und Kommunikationstechnologie bezieht.

Daher ist die Betriebsvereinbarung bei Bedarf für neu einzuführende Teile von IuK-Systemen bzw. für noch nicht geregelte Teile durch weitere zu vereinbarende Anlagen, z.B. betriebliche Richtlinien zu IuK-Systemen, zu ergänzen.

Diese Betriebsvereinbarung einschließlich aller Anlagen gilt für alle Mitarbeiter/innen sowie Arbeitsbereiche der MVHS.

Die MVHS wird dafür Sorge tragen, dass darüber hinaus alle Nutzer/innen der administrativen Infrastruktur der MVHS sich an die hier und in den Anlagen festgelegten Grundsätze halten.

3. Dokumentation

Die erteilten Zugriffsrechte werden dokumentiert.

Dieser Betriebsvereinbarung zugehörig ist eine Dokumentation, in der alle im Einsatz befindlichen IuK-Systeme verzeichnet sind. Aus ihr geht u. a. hervor

- der Name des IuK-Systems,
- in Stichworten eine Beschreibung des Leistungsumfangs und des Einsatzgebietes (Unternehmen/Betriebsstätte, Organisationsbereich, Funktion)
- das Betriebssystem.

Diese Dokumentation wird online im Intranet der MVHS geführt und jeweils ab dem Einsatzzeitpunkt neuer Systeme aktualisiert.

4. Grundsätze für Einführung, Einsatz und Änderungen von IuK-Systemen

Der Betriebsrat wird so rechtzeitig und umfassend schriftlich über alle Vorhaben, die sich mit Planung, Einführung, Einsatz und Änderungen von IuK-Systemen befassen, unterrichtet, dass eine Veränderung der Planung und Durchführung noch möglich ist (§ 80, Absatz 2 BetrVG). Er wird zu allen von der MVHS dazu einberufenen Arbeits- und Projektgruppen eingeladen.

Der Betriebsrat hat nach §92a BetrVG jederzeit ein Vorschlagsrecht zur Sicherung und Förderung der Beschäftigung.

Das Mitbestimmungsrecht des Betriebsrates ergibt sich unter anderem aus dem präventiven Schutz der Persönlichkeitsrechte der Mitarbeiter/innen (BetrVG § 75, Absatz 2). Der Betriebsrat hat darüber hinaus Informations-, Mitgestaltungs- und Mitbestimmungsrechte, insbesondere geregelt in den §§ 80,87,90,91, 92a, 106 und 111 BetrVG.

Die MVHS stellt sicher, dass alle von der Änderung der Arbeitsabläufe betroffenen Mitarbeiter/innen rechtzeitig informiert werden.

Geschäftsführung und Betriebsrat sind sich einig, dass alle notwendigen Qualifizierungsmaßnahmen unter vorheriger Beteiligung des BR rechtzeitig und umfassend durchgeführt werden (§§ 96 ff. BetrVG).

5. Schutz der Persönlichkeitsrechte

Daten, die für statistische Auswertungen genutzt werden, sind grundsätzlich in anonymisierter Form zu verwenden. Alle Ausnahmen sind mit dem Betriebsrat vorher zu vereinbaren.

Es besteht Einigkeit darüber, dass die Systeme nicht zum Zwecke der Leistungs- und Verhaltenskontrolle angewandt werden dürfen. Soweit bei der Benutzung der Systeme personenbezogene/-beziehbare Daten verarbeitet oder genutzt werden, die eine Aussage über die Leistung oder das Verhalten von Beschäftigten zulassen, dürfen diese nicht als Grundlage für personelle oder disziplinarische Maßnahmen herangezogen bzw. nutzbar gemacht werden.

Personenbezogene Erkenntnisse und arbeitsrechtliche Maßnahmen, die auf Erkenntnissen beruhen, die unter Verletzung der Bestimmungen dieser Betriebsvereinbarung gewonnen wurden, sind unwirksam. Die Verarbeitung oder Nutzung solcher personenbezogenen oder personenbeziehbaren Daten zu arbeitsrechtlichen Zwecken und insbesondere die Verarbeitung oder Nutzung solcher personenbezogenen oder personenbeziehbaren Daten im arbeitsgerichtlichen Urteilsverfahren ist unzulässig.

6. Verfahren bei Verdacht auf Verstöße

Nur bei begründeten und schriftlich zu dokumentierenden Verdachtsfällen auf Verstoß gegen die Regelungen dieser Rahmenbetriebsvereinbarung kann eine Verhaltenskontrolle auf Antrag der Geschäftsleitung oder des Betriebsrats und nur nach vorheriger Zustimmung der jeweils anderen Partei stattfinden. Das Ergebnis der Überprüfung ist vor der Einleitung von Maßnahmen mit dem Betriebsrat zu erörtern. Der/die einzelne Mitarbeiter/in hat in einem solchen Fall gemäß den gesetzlichen Bestimmungen das Recht auf Einsicht und Erläuterungen erfasster und ausgewerteter Daten, die seine/ihre Person betreffen.

Bei Vorliegen eines begründeten Straftatbestands besitzt §32 BDSG Gültigkeit. D.h. zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines/einer Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der/die Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des/der Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

7. Verwendung von Protokolldateien

Allen Beschäftigten wird bekanntgegeben, dass die Einzelverbindungsnachweise der Telefonanschlüsse und Diensthandys Verbindungsdaten enthalten (teilweise um die letzten Ziffern gekürzt).

Aufzeichnungen und Auswertungen der System- oder systemnahen Software über Benutzeraktivitäten (Login/Logout, aufgerufene Transaktionen, verbrauchte Systemressourcen, Zugang zu PC-Netzwerkservern, Intranet und Internet usw.) dürfen ausschließlich zu den folgenden Zwecken benutzt werden:

- Gewährleistung der Systemsicherheit,
- Abrechnung der Rechnerleistung, soweit vorgesehen
- Analyse und Korrektur von technischen Fehlern im System,
- Optimierung der Systeme

Der Zugriff auf die entsprechenden Funktionen wird auf das Personal des EDV-Bereichs begrenzt.

Allen Mitarbeitern/innen wird bekannt gegeben, dass alle Zugriffe auf das Internet durch das System protokolliert werden. Das Protokoll dient ausschließlich zur Gewährleistung der Systemsicherheit und zur Analyse und Korrektur von technischen Fehlern im System. Der Zugriff auf das Protokoll ist auf das Personal des EDV-Bereichs, das für die Aufrechterhaltung der Netz-Infrastruktur verantwortlich ist, beschränkt. Diese Personen dürfen die ihnen aus dem Protokollzugriff bekannt gewordenen Informationen nicht weitergeben.

Bei begründetem Verdacht auf missbräuchliche Nutzung des Internet-Zugangs gilt Ziffer 6 dieser Betriebsvereinbarung.

8. Zugriff auf Arbeitsplatzrechner

Soweit mittels Software zur Unterstützung der Netzwerkverwaltung ein Zugriff auf die Arbeitsplatzrechner von Mitarbeitern/innen möglich ist, wird dafür gesorgt, dass nur das berechtigte Administrationspersonal Zugriff auf die Endgeräte haben kann. Arbeitet der/die Mitarbeiter/in aktiv am Gerät, darf der Fernzugriff auf das Gerät nur durch vorherige Zustimmung des/der Mitarbeiters/in erfolgen. Der Zugriff kann jederzeit durch den/die Mitarbeiter/in beendet werden.

9. Arbeitsplatzgestaltung

Die von der Einführung von IuK-Systemen betroffenen Arbeitsplätze einschließlich deren Arbeitsumgebung müssen dem aktuellen Stand arbeitsphysiologischer, arbeitsmedizinischer und ergonomischer Erkenntnisse ebenso entsprechen wie allen anderen gesetzlichen und tariflichen Vorschriften und Betriebsvereinbarungen zum Schutz der Beschäftigten.

Die anfallenden Tätigkeiten werden unter Berücksichtigung der betrieblichen Möglichkeiten, der persönlichen Fähigkeiten und wirtschaftlichen Zweckmäßigkeit so verteilt, dass die den Arbeitnehmern/innen übertragenen Aufgaben ganzheitlich bearbeitet werden können, d.h. dass ein Höchstmaß an Arbeitsinhalten und Qualifikationen beim einzelnen Arbeitnehmer/bei der einzelnen Arbeitnehmerin liegt.

10. Absicherung gegen negative soziale Folgen

Es gelten die Vorschriften des Rationalisierungsschutztarifvertrages.

Die MVHS verpflichtet sich, Mitarbeiter/innen, deren Arbeitsplätze durch die Einführung der IuK-Systeme unmittelbar wegfallen, im Rahmen aller vorhandenen Möglichkeiten so zu versetzen, dass sie vorrangig gleichwertige Arbeiten unter Wahrung des sozialen Besitzstandes erhalten.

Die gesetzlichen Beteiligungs- bzw. Mitbestimmungsrechte, insbesondere nach §§ 99 ff; 111 ff. BetrVG bleiben hiervon unberührt.

11. Internet und Intranet

Der zentral gesicherte Zugang zum Internet wird im Rahmen der betrieblichen Aufgaben zur Verfügung gestellt und die private Nutzung ist grundsätzlich nicht erlaubt. Alles Weitere wird in den Anlagen geregelt.

Der Internet-Zugang darf nicht für rassistische, sexuell belästigende oder diskriminierende, rechtswidrige oder gegen die Systemsicherheit gerichtete Aktivitäten genutzt werden. Diese Regelungen gelten analog für die Intranetnutzung.

Der Betriebsrat hat das Recht, seine Arbeit betriebsöffentlich im Intranet darzustellen.

12. Nutzung von E-Mail und Outlook

Jeder Mitarbeiter hat das Recht, die Zugriffsrechte auf die Funktionen von Microsoft Outlook (Kalender, Aufgaben, Journal) selbst zu steuern (siehe Anlage). Outlook wird mit der Einstellung „alle Rechte beim Benutzer" ausgeliefert.

E-Mail wird als Betriebsmittel und nur zu dienstlichen Zwecken zur Verfügung gestellt. Eine private Nutzung ist grundsätzlich nicht erlaubt. Alles Weitere insbesondere die Zugriffs- und Vertretungsrechte wird in Anlagen geregelt.

Personenbezogene Daten und vertrauliche Inhalte die nicht durch Passwortschutz gesichert sind, dürfen nicht per E-Mail versendet werden. Das Bundesdatenschutzgesetz definiert in § 3: „Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person." Unter personenbezogenen Daten werden also allgemein alle Informationen verstanden, über die irgendwie ein Personenbezug hergestellt und eine (konkrete) Person somit direkt oder indirekt identifiziert werden kann. Vertrauliche Inhalte sind Informationen und Nachrichten, die nur für eine bestimmte Person oder einen beschränkten Empfängerkreis vorgesehen sind. Sie sind durch Rechtsnormen geschützt. (Z.B. Fernmelde- und Briefgeheimnis, Schweigepflicht von Ärzten und Rechtsanwälten etc.).

Ab dem Zeitpunkt, ab dem eine Verschlüsselungstechnik installiert ist, ist diese für den Versand personenbezogener Daten und vertraulicher Inhalte anzuwenden. Die Beschäftigten sind im Umgang mit der Verschlüsselungstechnik und dem Umgang mit personenbezogenen Daten bzw. vertraulichen Inhalten im Sinne des Bundesdatenschutzgesetzes vorher entsprechend zu schulen/unterweisen.

In Zweifelsfällen ist der/die Datenschutzbeauftragte der MVHS zu kontaktieren.

13. Schlussbestimmungen

Diese Betriebsvereinbarung tritt am 01.06.2016 in Kraft und ersetzt die bestehende Rahmenvereinbarung vom 14.01.2003.

Sie wird im MVHS-internen Intranet zusammen mit den jeweils gültigen Anlagen und Zusätzen veröffentlicht.

Die Betriebsvereinbarung kann mit einer Frist von 6 Monaten gekündigt werden. Geschäftsführung und Betriebsrat verpflichten sich in diesem Fall, unverzüglich Verhandlungen aufzunehmen und binnen einer Frist von 12 Monaten eine neue Vereinbarung abzuschließen. Ergänzungen und Änderungen auch in den Anlagen bedürfen der Zustimmung beider Parteien. Die Betriebsvereinbarung wirkt bis zum Abschluss einer neuen Betriebsvereinbarung nach.

München, den

Prof. Dr. Klaus Meisel	**Dr. Susanne May**	**Rita Schösser**
Managementdirektor	**Programmdirektorin**	**Betriebsratsvorsitzende**

Anlagen zur Rahmenbetriebsvereinbarung über die Einführung und den Einsatz von Informations- und Kommunikationssystemen (IuK) an der Münchner Volkshochschule

Anlage 1: Kennwortsicherheit für die Anmeldung am System

Die EDV-Revision hat eine erhöhte Kennwortsicherheit für die Anmeldung am System gefordert. Um diese Vorgaben zu erfüllen, gelten nachfolgende Richtlinien:

- Die minimale Kennwortlänge beträgt 8 Zeichen.
- Das Kennwort muss eine bestimmt Komplexität aufweisen. Dabei müssen mindestens drei der folgenden Kriterien erfüllt sein:
  - Großbuchstabe A bis Z
  - Kleinbuchstabe a bis z
  - Ziffern 0 bis 9
  - nicht alphanumerische Zeichen wie + - ? ! (Kennwortbeispiele: *Unter(tasse)* oder *MoDiMiDo!* oder *Keller-str*).
- Das Kennwort darf nicht drei oder mehr Zeichen in Folge aus dem Anmeldename des Benutzers enthalten.
- Das Kennwort gilt mindesten 1 Tag und muss spätestens alle 42 Tage geändert werden. Hierzu werden Sie automatisch rechtzeitig aufgefordert.
- Die letzten drei Kennwörter dürfen wegen der Kennwortchronik nicht wiederverwendet werden.
- Das Kennwort ist nicht an Dritte weiterzugeben oder offen am Arbeitsplatz zu hinterlegen.

Geben Sie Ihr Kennwort 3 Mal in einem Zeitraum von einer halben Stunde fehlerhaft ein, wird Ihr Anmeldekonto gesperrt. Im Falle einer Sperre wird Ihr Benutzerkonto automatisch nach 15 Minuten wieder entsperrt.

Haben Sie Ihr Passwort vergessen, kann der Benutzerservice ein temporäres neues Kennwort zur Verfügung stellen. Dieses temporäre Kennwort ist sofort vom Mitarbeiter/von der Mitarbeiterin nach den o.g. Richtlinien zu ändern.

Die Sperre des Benutzerkontos kann ebenfalls durch den Benutzerservice aufgehoben werden.

Anlage 2: Elektronische Post

a) Regeln zur E-Mail-Kommunikation

Die Geschäftsführung und der Betriebsrat haben verbindliche Regeln zur E-Mail-Kommunikation festgelegt:

1. **Klare und überlegte Adressierung**
   - Einzig die Person(en) unter „An" ist/sind aufgefordert zu reagieren.
   - Die Person(en) in „CC" wird/werden nur in Kenntnis gesetzt, z.B. wenn der Sachverhalt es unbedingt erfordert bzw. darum gebeten wurde.
   - „BCC" wird intern nicht verwendet. Bei Anschreiben an mehrere externe Kommunikationspartner ist „BCC" zulässig, um den Datenschutz zu gewährleisten.
   - E-Mails „an alle Mitarbeiter" nur nach Genehmigung der Programmbereichsleitungen bzw. der Geschäftsführung (Ausnahme: Betriebsrat).
   - Auf die Anwendung von Lese- bzw. Empfangsbestätigungen wird verzichtet.
   - Nur in Ausnahmefällen wird die Wichtigkeit von E-Mails über „hoch" oder „rotes Fähnchen" markiert, z.B. bei zeitlicher Dringlichkeit.
2. **Aussagekräftiger Betreff, Länge der Nachricht und klarer Auftrag**
   - Der Betreff benennt prägnant das Thema der E-Mail.
   - Informationen werden kurz und knapp formuliert.
   - Ein klarer Auftrag wird formuliert, z.B. Bitte um Terminvereinbarung.
3. **Einhalten der Höflichkeitsformen**
   - Anrede- und Grußformeln aus der Briefkommunikation werden eingehalten.
   - Auf mehrfache Ausrufungszeichen (!!!) und KAPITÄLCHEN wird verzichtet.
   - Nachrichten sind freundlich, unmissverständlich und sachlich zu formulieren.
4. **Signatur**
   - Es ist eine E-Mailsignatur nach den Richtlinien der EDV (s. Intranet) einzurichten.
   - Im Erstkontakt ist die Signatur stets zu verwenden, innerhalb anhaltendem E-Mailverkehr ist auf die Signatur zu verzichten (bessere Lesbarkeit).
5. **Größe, Benennung und Form von Anhängen**
   - Dateien haben aussagekräftige Titel und ein gängiges Format (.doc, .pdf, .jpg).
   - Dateien, die nicht mehr bearbeitet werden sollen, haben pdf-Format.
   - Sehr große Dateianhänge werden komprimiert (z.B. als zip-Datei) versendet.
6. **Dienstliche Nutzung, Vertraulichkeit und Datenschutz**
   - Outlook wird grundsätzlich nur für dienstliche Belange genutzt.
   - Sensible Daten, die nicht durch Passwortschutz gesichert sind, dürfen nicht per E-Mail versendet werden. Ab dem Zeitpunkt, ab dem eine Verschlüsselungstechnik im Betrieb installiert ist, ist diese für den Versand sensibler Daten anzuwenden. Die Mitarbeiter und Mitarbeiterinnen werden entsprechend geschult und erhalten eine Information zur Handhabung. Die Vertraulichkeit von E-Mails wird bei der Weiterleitung berücksichtigt (ggf. die Zustimmung des Absenders einholen).
7. **Abwesenheits-, Zugriffs- und Vertretungsregelungen**

- Bei vorhersehbarer Abwesenheit (z.B. Urlaub, Dienstreise, Gleitzeit) von mehr als 3 Tagen richtet der/die Mitarbeiter/in einen Abwesenheitsassistenten ein, der die Zeit der Abwesenheit und eine Vertretungs- bzw. Weiterleitungsregel benennt.
- Jede/r Mitarbeiter/in ist aufgefordert, eine Postfach-Stellvertretung festzulegen (in der Regel analog der bestehenden Urlaubs- und Krankheitsvertretung). Bei Abwesenheit ist die Stellvertretung befugt, auf das Email-Konto zuzugreifen und wichtige E-Mails zu bearbeiten. Die Stellvertretungsregelung ist schriftlich zu dokumentieren und von dem/der Vorgesetzten aufzubewahren. Die Dokumentation muss aktuell sein, etwaige Änderungen oder Ergänzungen sind zu berücksichtigen.
- Wird keine Postfach-Stellvertretung eingerichtet, ist bei Krankheit wie folgt zu verfahren: Der EDV-Benutzerservice wird vom/von der Vorgesetzten des Mitarbeiters/der Mitarbeiterin umgehend über die Abwesenheit per Mail informiert und schaltet den Abwesenheitsassistenten ein, sofern nicht bereits vom Mitarbeiter/von der Mitarbeiterin ein Abwesenheitsassistent aktiviert wurde. Bei Wiederaufnahme der Arbeit ist ein neues Kennwort einzugeben.

8. Zeitnahe Beantwortung und Terminvereinbarungen

- In der Regel werden Anfragen innerhalb von drei Tagen beantwortet.
- Terminabsprachen oder das Setzen von angemessenen Fristen sind erwünscht.

9. Vorzüge des telefonischen und persönlichen Gesprächs

- Bei zeitlicher Dringlichkeit, Vertraulichkeit der Inhalte oder bei langen Ausführungen ist das persönliche Gespräch oder ein Telefonat vorzuziehen.

10. E-Mail-freie Zeit

- Es besteht keine Pflicht am Wochenende, nach Beendigung der individuellen Arbeitszeit oder in Urlaubs- oder Krankheitszeiten E-Mails zu schreiben oder zu lesen.
- E-Mail-freie Phasen innerhalb eines Arbeitstages sind einzuplanen.

b) Speicherkapazität E-Mailfach

Jedes persönliche Postfach hat eine begrenzte Speicherkapazität, die für eine normale Nutzung vollkommen ausreicht. Ist diese Grenze erreicht, erfolgt automatisch eine Warnmeldung mit der Aufforderung zur Löschung von Daten. Dieser Aufforderung ist umgehend nachzukommen. Es erfolgt keine Erweiterung der Speicherkapazitäten der persönlichen Postfächer.

Eine Erhöhung der Speicherkapazität ist nur in Ausnahmefällen und dann nur für Bereichs- oder Projektpostfächer möglich. In den Projektbereichen ist die Sonderregelung mit der mehrjährigen Archivierungspflicht begründet. Die Erhöhung der Speicherkapazität wird nur mit vorliegender Genehmigung durch den/die Leiter/in des Zentralen Services durchgeführt.

Diese Regelungen sind für alle Mitarbeiter/innen der MVHS verbindlich einzuhalten.

Anlage 3: Zugriff über das Internet auf MVHS-interne Arbeitsumgebung

Präambel:
Die MVHS legt Wert darauf, dass Freizeit auch Freizeit ist. Dauernde Verfügbarkeit sowie das Schreiben und Beantworten von E-Mails nach Dienstschluss ist ausdrücklich nicht gewünscht. Der erweiterte und passwortgeschützte Zugriff über das Internet (z.B. über private Endgeräte von zu Hause aus oder von unterwegs) auf MVHS-eigene IuK-Systeme und Dateien ist deshalb nur unter bestimmten Bedingungen möglich und wird nach Bedarf bereitgestellt. Folgende abgestuften Nutzungsbedingungen und Genehmigungswege sind einzuhalten:

1. **Zugriff auf elektronischen Kalender, E-Mail-Postfach und Intranet:**
   - Dieses Service-Angebot steht bis auf Weiteres allen MitarbeiterInnen der MVHS zur Verfügung und kann ohne Zustimmung der/des Vorgesetzten genutzt werden.
   - Eine Synchronisierung mit privat genutzten Outlook-Systemen ist hierbei jedoch nicht gestattet, da MVHS-Ressourcen ausschließlich für betriebliche Nutzungen zur Verfügung stehen und es nicht zu einer Vermischung privater und dienstlicher Belange kommen soll.

2. **Zugriff auf die eigene MVHS-interne Arbeitsumgebung:**
   - Diese Zugriffsart steht nur bestimmten MitarbeiterInnen der MVHS nach begründeter Genehmigung der direkten Vorgesetzten zur Verfügung. Die Vorgesetzten leiten die begründete Genehmigung per E-Mail an den EDV-Benutzerservice zur Umsetzung weiter.
   - Eine Beantragung und Genehmigung bezieht sich auf einen temporären Zugriff, z.B. für MitarbeiterInnen der MVHS, die im Rahmen einer Dienstreise oder Fortbildung zeitlich begrenzt von außerhalb der Büroräume auf Daten zugreifen müssen.
   - BR-Mitglieder beantragen den Zugriff auf die Arbeitsumgebung des BR bei der/dem BR-Vorsitzenden.

3. **Home-Office-Arbeitsform mit Zugriff auf die eigene MVHS-interne Arbeitsumgebung:**
   - Home-Office bedeutet, dass MitarbeiterInnen der MVHS permanent oder auf einen definierten Zeitraum begrenzt auch während der Kernarbeitszeiten von zu Hause aus arbeiten dürfen.
   - Permanenter Zugriff: z.B. für MitarbeiterInnen der MVHS, die gelegentlich, aber immer wieder und aus unabdingbaren Gründen auch außerhalb der Kernarbeitszeit Dateien einsehen und bearbeiten müssen (z.B. EDV-MitarbeiterInnen).
   - Begrenzt auf einen definierten Zeitraum: Ausschließlich Ausnahmefälle begründen die Genehmigung, wie z.B. Pflege eines Angehörigen oder Betreuung von Kindern.
   - Es besteht weder ein Anspruch auf die Home-Office-Arbeitsform noch auf eine technische Ausstattung durch die MVHS bei Genehmigung.
   - Die Beantragung erfolgt durch die MitarbeiterInnen und wird zusammen mit einer Stellungnahme des/der Vorgesetzten an die Personalleitung weitergeleitet, die den Antrag zur Genehmigung der Geschäftsführung (Managementdirektor) vorlegt.

Für alle drei Zugriffsstufen gilt:
- Eine Pflicht zur Nutzung für die MitarbeiterInnen der MVHS besteht nicht und kann nicht eingefordert werden.
- Die jährliche zu unterzeichnende Lesebestätigung dieser Rahmenbetriebsvereinbarung sichert die regelmäßige Kenntnisnahme der Sicherheitsregelungen.

Sie werden im jährlichen Turnusschreiben über die Personalabteilung dazu aufgefordert. Anlage 6 (Nutzungsbedingung für IT-Dienste) gilt es insbesondere zu beachten.

- Jeder Mitarbeiter und jede Mitarbeiterin ist verpflichtet, die ihm oder ihr im Rahmen des Vertragsverhältnisses und seiner Tätigkeit bekannt gewordenen Daten, Informationen und Dokumente zeitlich unbegrenzt, insbesondere auch über die Dauer des Vertragsverhältnisses hinaus, streng vertraulich zu behandeln. Derartige Informationen dürfen Dritten nicht zugänglich gemacht oder weitergegeben werden, außer in Erfüllung der vertraglichen Pflichten.

Anlage 4: Elektronische Terminverwaltung

An der MVHS ist es eine betriebliche Notwendigkeit, Terminabstimmungen vorzunehmen. Hierfür steht jedem Mitarbeiter und jeder Mitarbeiterin ein elektronischer Kalender (z.B. Microsoft Outlook System) als Arbeitsmittel zur Verfügung.
Alle Termine und Abwesenheitszeiten innerhalb der individuell vereinbarten Arbeitszeit müssen in den elektronischen Kalender eingetragen werden, um diesen als Planungsinstrument, z.B. für Team- und Projekttreffen nutzen zu können. Der verpflichtend zu nutzende Kalender wird dabei nur als Planungs- und Koordinierungsinstrument genutzt, nicht jedoch zur Dokumentation der tatsächlichen Arbeitszeit. Insbesondere besteht keine Verpflichtung, Kalendereinträge nachträglich zu korrigieren, wenn das tatsächliche Geschehen von der Planung abweicht. Die Sichtbarkeit der Termine für andere Kollegen und Kolleginnen beschränkt sich ausschließlich auf eine rein visuelle Darstellung der Verfügbarkeit bzw. Nichtverfügbarkeit, um gemeinsame „Zeitfenster" für eine ausstehende Terminplanung ausmachen zu können. Die Benennung der Termine sowie die Ortsangaben von Terminen bleiben in einem nicht öffentlichen Status.
Vorgesetzte, jede Mitarbeiterin und jeder Mitarbeiter haben das Recht, andere Personen zu Terminen einzuladen. Eine Möglichkeit, Termine für andere Personen ohne deren vorherige Einwilligung einzutragen, wird technisch jedoch nicht zur Verfügung gestellt.

Für den Umgang mit dem elektronischen Outlook-Kalender werden jedem Mitarbeiter und jeder Mitarbeiterin nach Bedarf Schulungen angeboten.

Anlage 5: Leitfaden für den dienstlichen Umgang mit sozialen Medien (Stand 27.05.2014)

Grundlage und Hauptquelle: „Social Media Guideline. Leitfaden für den Umgang mit sozialen Medien der Landeshauptstadt München"

Social-Media-Portale wie Facebook, YouTube, Twitter aber auch Foren und Blogs bieten neue Wege, um sich auszutauschen. Damit ist nicht nur die Kommunikation zwischen Kolleginnen und Kollegen in der MVHS gemeint, sondern auch der Austausch und die Diskussion mit und zwischen Kursleiterinnen/Kursleitern, mit Teilnehmerinnen/Teilnehmern und mit Bürgerinnen/Bürgern. Auch wenn für Volkshochschulen nach wie vor die Stärke im Präsenzlernen und im „Vor-Ort-sein" liegt, weiß die MVHS um die Bedeutung sozialer Netzwerke und wie diese die öffentliche Wahrnehmung der MVHS beeinflussen.

Um Sie in einem sicheren und verantwortungsvollen Umgang mit Blogs, Foren und sozialen Netzwerken zu unterstützen und als öffentliche Einrichtung klar Position zu beziehen, hat die MVHS sich dazu entschlossen, im Rahmen einer Social Media Guideline Empfehlungen für den Umgang mit sozialen Medien zu geben. Denn die MVHS trägt eine besondere gesellschaftliche Verantwortung. Sie ist sich der Chancen und der Risiken, die mit Social Media Portalen einhergehen, bewusst. Datenschutz, Privatsphäre, Urheberrechte, aber auch der respektvolle Umgang miteinander sind wesentliche Elemente, die im Umgang mit Social Media eingehalten werden sollten. Jeder, der sich online über die MVHS äußert, prägt damit ihr Bild in der Öffentlichkeit.

Für einen sicheren und verantwortungsvollen Umgang mit Blogs, Foren und sozialen Netzwerken bitten wir Sie folgendes zu beachten:

1. Bei einer Nutzung des Internets über Rechner der MVHS gilt diese „Rahmenbetriebsvereinbarung über die Einführung und den Einsatz von Informations- und Kommunikationssystemen an der Münchner Volkshochschule".
2. Alle Kolleginnen und Kollegen, die befugt sind, Social-Media-Portale zu Dienstzwecken offiziell zu nutzen (z.B. Pflege des offiziellen Facebook-Auftritts der MVHS), erhalten eine Schulung. Das Ziel solcher Schulungen ist es, einen sensiblen und verantwortungsvollen Umgang mit Social-Media-Portalen zu lernen.
3. Die MVHS bietet im mediendidaktischen Kursprogramm für Kursleiterinnen und Kursleiter sowohl für die Moodle-Plattform als auch für den Umgang mit anderen Social-Media-Portalen und -Netzwerken regelmäßig Schulungen an, die selbstverständlich auch von allen Mitarbeiterinnen und Mitarbeitern der MVHS wahrgenommen werden können.
4. Alle Fachgebietsleitungen haben die Aufgabe ihre Kursleiterinnen und Kursleiter zu sensibilisieren. Hierfür steht ihnen die „Social Media Guideline für Kursleitungen" zur Verfügung sowie der Verweis auf mediendidaktische Schulungen der MVHS (vgl. Punkt 3).
5. Betriebsinterne Informationen über die Münchner Volkshochschule jeglicher Art, insbesondere über Personalangelegenheiten, sind vertraulich zu behandeln und in keinem Fall zu veröffentlichen oder Dritten bekannt zu machen.
6. Offizielle Statements oder Erklärungen der MVHS werden nur von autorisierten Mitarbeiterinnen und Mitarbeitern veröffentlicht.
7. Achten Sie auf die Einhaltung des Urheberrechts und veröffentlichen Sie nur Bilder, Texte und Videos, bei denen die Rechte eindeutig geklärt sind. Urheberechtlich dürfen keine Bilder von Personen online gestellt werden, deren schriftliche Einwilligung hierzu nicht vorliegt. Seien Sie auch mit der Nennung von Namen vorsichtig.

8. Seien Sie im Netz in jedem Fall höflich und respektvoll. Sollte Ihnen im Umgang mit dem Internet einmal ein Fehler unterlaufen sein (z.B. Angabe eines falschen Veranstaltungsortes), stehen Sie dazu und ändern oder ergänzen Sie Ihre Beiträge - möglichst bevor Missverständnisse entstehen.
9. Soziale Medien dürfen nicht für rassistische, sexuell belästigende oder diskriminierende, rechtswidrige oder gegen die Systemsicherheit gerichtete Aktivitäten genutzt werden.

Anlage 6:. Umgang mit firmeneigenen IT-Geräten (z.B. Smartphone) und Nutzungsbedingungen für IT-Dienste

In Bezug auf den Umgang mit firmeneigenen IT-Geräten ist die Dienstanweisung Nr. A 5 zu beachten.

Für die Nutzung aller IT-Dienste gilt:

- Die Ressourcen stehen ausschließlich für die betriebliche Nutzung der MVHS zur Verfügung. Eine private Nutzung ist grundsätzlich nicht erlaubt. Die Weitergabe der Zugangsdaten an Dritte ist ausdrücklich untersagt. Gelangen andere Personen als die/der Berechtigte an die Zugangsdaten (z.B. bei Verlust eines IT-Gerätes) ist unverzüglich der Benutzerservice bzw. die Systemadministration der MVHS zu verständigen.
- Werden MVHS-IT-Dienste auf MVHS-fremden Geräten genutzt, ist darauf zu achten, dass ein aktuelles Antiviren-Programm eingesetzt und für alle eingesetzten Programme und Tools die aktuellen Betriebssystem- und Internet-Browser-Sicherheitspatches installiert sind.
- Beim Umgang mit Datenträgern und IT-Geräten ist speziell darauf zu achten, dass der Schutzbedarf der Informationen hinsichtlich der Vertraulichkeit gewahrt bleibt. Die Entsorgung von Datenträgern und IT-Geräten ist durch den Benutzerservice vorzunehmen.
- In Bereichen mit Besucherverkehr ist sicherzustellen, dass IT-Systeme nicht unbeaufsichtigt sind oder entsprechend gesperrt werden.
- Bei der Verwendung mobiler Endgeräte ist besondere Sorgfalt erforderlich. Sie dürfen zu keiner Zeit für Dritte frei und unbeaufsichtigt zugänglich sein. Beim Aufenthalt in unsicheren Umgebungen bzw. in der Öffentlichkeit ist darauf zu achten, dass sensible Informationen nicht durch Mithören oder Mitlesen ausgespäht werden können. Beim Verlassen des Arbeitsplatzes ist die Bildschirmsperre zu aktivieren.

Jeder Mitarbeiter und jede Mitarbeiterin ist verpflichtet, die ihm oder ihr im Rahmen des Vertragsverhältnisses und seiner Tätigkeit bekannt gewordenen Daten, Informationen und Dokumente zeitlich unbegrenzt, insbesondere auch über die Dauer des Vertragsverhältnisses hinaus, streng vertraulich zu behandeln. Derartige Informationen dürfen Dritten nicht zugänglich gemacht oder weitergegeben werden, außer in Erfüllung der vertraglichen Pflichten.

Anlage 7: Richtlinien zur Softwareinstallation

Grundsätzlich sind nur für die IT-Nutzung freigegebene IT-Systeme einzusetzen.

Im EDV-Netzwerk des Unternehmens und besonders auf allen Servern, Computern Laptops, Smartphones, Tabletts etc. dürfen nur Softwareprodukte installiert und genutzt werden, die von der Geschäftsleitung bzw. vom/von der Sachgebietsleiter/in EDV genehmigt wurden und die rechtmäßig lizenziert sind.

Mitarbeiter dürfen keine Software aus dem Internet herunterladen oder auf anderem Weg auf Computern des Unternehmens installieren oder direkt starten. Dazu gehören auch Bildschirmschoner, Demoprogramme, Computerspiele oder Utilities.

Die vorgegebene Arbeitsplatzkonfiguration darf vom IT-Nutzer nicht verändert werden. Ausgenommen von dieser Vorgabe sind lediglich Softwareeinstellungen für die in der bereitgestellten Arbeitsumgebung Konfigurationsmöglichkeiten zur Verfügung stehen.

Anlage 8: Übergaberegelungen beim Ausscheiden aus der MVHS

Vor Verlassen der MVHS stellt der Mitarbeiter/die Mitarbeiterin in Zusammenarbeit mit dem EDV-Benutzerservice sicher, dass der Vorgesetzte/die Vorgesetzte bzw. der Nachfolger/die Nachfolgerin einen Zugang zum Homelaufwerk bekommt.

Für das E-Mail-Konto muss durch den EDV-Benutzerservice eine Benachrichtigung für mindestens 6 Wochen und maximal 2 Monate eingestellt werden, die auf den Vorgesetzten/die Vorgesetzte bzw. den Nachfolger/die Nachfolgerin verweist. Zusätzlich erhält der/die Vorgesetzte oder ein/e von ihm/ihr Bevollmächtigte/r bzw. der/die Nachfolger/in Zugriff auf das E-Mail-Konto. Danach ist das Konto zu löschen.

Bei Betriebsratsmitgliedern ist der Zugriff auf das E-Mail-Konto nur nach vorheriger Prüfung und mit Zustimmung zur Löschung durch den Betriebsrat zulässig.