MAX-PLANCK-INSTITUT
FÜR MULTIDISZIPLINÄRE
NATURWISSENSCHAFTEN

Nutzungsordnung für die IT-Dienste des Max-Planck-Instituts für Multidisziplinäre Naturwissenschaften (MPI-NAT)

Ziel

Aufgabe des Instituts ist es, eine leistungsfähige, zuverlässige, sichere, und gesetzeskonforme IT-Infrastruktur im Dienste der Wissenschaft einzurichten und zu betreiben. Dazu bedarf es der Kooperation und aktiven Mitarbeit aller Nutzer*innen, die durch diese Nutzungsordnung verbindlich festgeschrieben wird.

Geltungsbereich

- Die Nutzungsordnung gilt für die Nutzung der IT-Infrastruktur, bestehend aus Netzwerk, IT-Systemen und Anwendungen an allen Standorten des MPI-NAT.
- Die Nutzungsordnung gilt auch für die dienstliche Nutzung privater IT-Geräte, sowie beim Einsatz dienstlicher Geräte außerhalb des Instituts.
- Alle Nutzer*innen der IT-Infrastruktur - unabhängig von der Art ihres Rechtsverhältnisses zum MPI-NAT - sind verpflichtet, die Regelungen dieser Nutzungsordnung einzuhalten.
- Bei Nutzung von Diensten, die durch andere Provider, wie z.B. die „Gesellschaft für Wissenschaftliche Datenverarbeitung mbH Göttingen“ (GWDG), bereitgestellt werden, gilt ergänzend deren Nutzungsordnung.
- Soweit gesetzliche Bestimmungen und/oder (Gesamt-)Betriebsvereinbarungen Rechte oder Pflichten für Beschäftigte der MPG abweichend von dieser Nutzungsordnung regeln, haben diese Regelungen Vorrang.

Nutzungsberechtigung und Zulassung zur Nutzung

- Nutzungsberechtigt sind alle Personen, die mit dem MPI-NAT einen laufenden Arbeits- oder Dienstvertrag, einen Gast- und Gestattungsvertrag haben oder die mit dem MPI-NAT in einem sonstigen vertraglichen Verhältnis stehen.
- Die Zulassung zur Nutzung erfolgt ausschließlich zur Erfüllung dienstlicher oder vertraglicher Aufgaben oder zu wissenschaftlichen Zwecken in Forschung, Lehre und Ausbildung. Hiervon abweichende Nutzungen regelt die Max-Planck-Gesellschaft.
- Die Zulassung zur Nutzung erfolgt auf Antrag und unter gleichzeitiger verbindlicher Anerkennung der Nutzungsordnung.
- Die Nutzungserlaubnis kann zeitlich befristet und auf bestimmte IT-Ressourcen eingeschränkt werden.

- Die Nutzungserlaubnis erlischt, wenn die vertragliche Grundlage ausläuft.
- Einer*einem Nutzer*in kann aus wichtigem Grund die Nutzungserlaubnis entzogen werden. Hierüber entscheidet die Institutsleitung. Der*dem betroffenen Nutzer*in soll vor dem Entzug der Nutzungserlaubnis Gelegenheit zur Stellungnahme gegeben werden, soweit die Zweckerreichung dadurch nicht gefährdet ist.

Pflichten der Nutzer*innen

Allgemein

- Die Nutzer*innen haben jedes rechtswidrige oder nach allgemein gültigen ethischen Maßstäben unangemessene Nutzungsverhalten zu unterlassen. Sie haben darüber hinaus jedes Nutzungsverhalten zu unterlassen, das geeignet ist, Nachteile für die Max-Planck-Gesellschaft oder das Institut herbeizuführen oder das Ansehen oder die Interessen der Max-Planck-Gesellschaft oder des Instituts zu schädigen oder zu verletzen.
- Vom Institut zur Verfügung gestellte Geräte sind pfleglich zu behandeln. Veränderungen an den Geräten müssen mit dem IT-Personal abgestimmt werden.

Meldung von IT-Problemen

- IT-Probleme jeglicher Art (Systemabstürze, fehlerhaftes Verhalten von Anwendungen, die bisher fehlerfrei liefen, Verdacht auf Eindringen von Unbefugten oder Schadsoftware im System) müssen dem IT-Personal unverzüglich gemeldet werden.

Installation von Software

- Auf den Rechnern des Instituts darf nur korrekt lizenzierte Software installiert werden, die für dienstliche Aufgaben erforderlich sind.
- Das Installieren und Ausführen von zusätzlicher Software durch Nutzer*innen ist nur nach erteilter Berechtigung gestattet.

Zugriffskontrolle

- Beim Verlassen des Arbeitsplatzes ist der Rechner gegen unberechtigte Zugriffe zu schützen („sperren“). Ausnahmen sind möglich, falls die Arbeitsorganisation es dringend erfordert (z.B. Mess- und Steuerrechner) und auf andere Weise sichergestellt ist, dass kein unberechtigter Zugriff erfolgen kann.
- Soweit technisch möglich, müssen Endgeräte durch Passwort, PIN, Fingerabdruck oder andere Verfahren vor unberechtigtem Zugriff geschützt werden.
- Die Speicherung von schützenswerten Daten auf Notebooks oder Speichermedien (wie USB-Sticks, externe Festplatten) ist nur dann zulässig, wenn die Medien oder die Daten verschlüsselt sind.

Umgang mit Zugangsdaten

- Geheimhaltung: Die eigenen, geheimen Zugangsdaten (Passworte, private Schlüssel) müssen vertraulich behandelt werden und dürfen keiner anderen Person mitgeteilt werden. Die Eingabe muss unbeobachtet stattfinden.
- Verdacht auf Kompromittierung: Bei Anzeichen einer möglichen Kompromittierung der Zugangsdaten müssen diese unverzüglich geändert und der IT-Service benachrichtigt werden.
- Starke Passwörter: Falls Passwörter zur Authentifizierung verwendet werden, sollten diese stark sein, d.h.

  - ausreichend lang (mindestens 10 Stellen), zufällig und komplex sein
  - auf keinen Sachverhalten basieren, die eine andere Person unter Zuhilfenahme personenbezogener Daten wie z. B. Namen, Telefonnummern, Geburtstage usw. einfach erraten oder erschließen kann
- Passwörter sollten
  - nicht im Klartext gespeichert oder notiert werden
  - sich für verschiedene Benutzerkonten unterscheiden; das gilt insbesondere für externe Konten
  - zweckmäßigerweise in einem Passwort-Manager generiert und verwaltet werden
  - bei der ersten Anmeldung geändert werden, wenn es sich um initiale Passwörter handelt
- Wenn die Möglichkeit zur 2-Faktor-Authentifizierung besteht, sollte diese genutzt werden.

E-Mail

- Für dienstliche E-Mail-Kommunikation ist nur die Verwendung dienstlicher E-Mail-Konten zulässig.
- Es muss sichergestellt werden, dass dienstliche E-Mails regelmäßig gelesen werden.
- Eine systematische Weiterleitung dienstlicher E-Mails an externe Provider oder der Zugriff eines externen Providers auf das dienstliche E-Mail-Konto sind nicht zulässig.
- Schützenswerte Daten dürfen nicht unverschlüsselt per E-Mail verschickt werden.
- Internetlinks und Attachments in E-Mails sollten nur dann geöffnet werden, wenn durch Herkunft und Kontext davon ausgegangen werden kann, dass sie vertrauenswürdig sind.

Umgang mit Daten

- Dienstliche Daten sind grundsätzlich auf IT-Systemen des Instituts, der GWDG oder anderen vom Institut zugelassenen IT-Systemen zu speichern. Falls es dienstlich erforderlich ist und die Daten nur normalen Schutzbedarf haben, können auch andere Systeme (externe Cloud-Dienste, private Geräte)-verwendet werden.
- Daten sollten möglichst auf den zentralen Fileservern gespeichert werden. Werden sie lokal oder auf anderen Servern gespeichert, muss insbesondere sichergestellt werden, dass sie regelmäßig gesichert werden (Backup).
- Eine Verarbeitung personenbezogener Daten mit erhöhtem Schutzbedarf muss mit der*dem Datenschutzkoordinator*in abgestimmt werden. Die Verantwortung für den Schutz der Daten und Programme auf den Anlagen des Instituts obliegt primär der*dem Nutzer*in als verantwortlicher Stelle. Diese*dieser ist bei der Verarbeitung personenbezogener Daten verpflichtet, geeignete Schutzmaßnahmen im Sinne der Datenschutzgesetze umzusetzen, wobei die IT des Instituts geeignete Schutzmaßnahmen zur Verfügung stellt.
- Beim Ausscheiden aus dem Institut müssen alle dienstlichen Daten dem bzw. der Vorgesetzten geordnet übergeben werden. Hierbei ist insbesondere die Einhaltung der “guten wissenschaftlichen Praxis” sicherzustellen, die fordert, dass Daten, die Grundlage von Publikationen sind, mindestens 10 Jahre im Institut aufgehoben werden müssen.
- Evtl. vorhandene nicht dienstliche Daten müssen in einem Ordner „PRIVATE“ liegen und vor dem Ausscheiden gelöscht werden.

Rechte des IT-Personals

Das IT-Personal mit erweiterten Rechten sind die benannten IT-Administrator*innen des „IT & Elektronik Service“ (nachfolgend „IT-Service“) und die IT-Beauftragten der Abteilungen und Arbeitsgruppen. Nur diese sind berechtigt:

- nach Ablauf der Nutzungsberechtigung alle Daten und Programme des Nutzers bzw. der Nutzerin zu sperren und zu löschen, sofern die Daten im Institut keine weitere Verwendung finden.
- soweit es zur Störungsbeseitigung, aus Gründen der Systemadministration und Systemsicherheit oder zum Schutz der Nutzerdaten erforderlich ist, die Nutzung von IT-Ressourcen vorübergehend einzuschränken oder einzelne Nutzerkennungen vorübergehend zu sperren. Sofern möglich, sind die betroffenen Nutzer*innen hierüber im Voraus zu unterrichten.
- die Inanspruchnahme der IT-Infrastruktur durch die einzelnen Nutzer*innen zu dokumentieren und auszuwerten, jedoch nur soweit dies erforderlich ist
  1. zur Gewährleistung eines ordnungsgemäßen Systembetriebs oder
  2. zur Ressourcenplanung und Systemadministration oder
  3. zum Schutz der personenbezogenen Daten anderer Nutzer oder
  4. zu Abrechnungszwecken oder
  5. für das Erkennen und Beseitigen von Störungen

  Dabei ist die Betriebsvereinbarung „Nutzung technischer Einrichtungen zur Überwachung von Arbeitsplatz-Computern“ zu berücksichtigen.
- die weitere IT-Nutzung zu verhindern, sofern Anhaltspunkte dafür vorliegen, dass ein*eine Nutzer*in die IT-Infrastruktur rechtswidrig nutzt. Dies jedoch längstens, bis die Rechtslage hinreichend geklärt ist.
- Einsicht in Nutzerdaten zu nehmen, soweit dies zur Beseitigung aktueller Störungen unbedingt notwendig ist.

Haftung des*der Nutzer*in

- Für die Haftung und die Freistellungspflichten von Nutzer*innen, die Beschäftigte der MPG sind, gelten die arbeitsvertraglich vereinbarten Haftungsregelungen bzw. die allgemeinen arbeitsrechtlichen Haftungsgrundsätze. Für Nutzer*innen, die keine Beschäftigten der MPG sind, gelten die nachstehenden Absätze.
- Die*Der Nutzer*in haftet für alle Schäden und Nachteile, die der MPG durch eine missbräuchliche oder rechtswidrige Verwendung der IT-Infrastruktur bzw. dadurch entstehen, dass die*der Nutzer*in schuldhaft ihren*seinen Pflichten aus dieser Nutzungsordnung nicht nachkommt.
- Die*Der Nutzer*in haftet für Schäden, die im Rahmen der ihr*ihm zur Verfügung gestellten Zugriffs- und Nutzungsmöglichkeiten durch Drittnutzung entstanden sind, wenn sie*er die Drittnutzung zu vertreten hat.
- Die*Der Nutzer*in hat die MPG von allen Ansprüchen freizustellen, die Dritte gegen die MPG aufgrund einer schuldhaften Verletzung ihrer*seiner Pflichten aus dieser Benutzungsordnung gelten machen.

Haftung des MPI-NAT

- Das MPI-NAT übernimmt keine Garantie dafür, dass die IT-Infrastruktur jederzeit fehlerfrei funktioniert. Eventuelle Datenverluste infolge technischer Störungen sowie

die Kenntnisnahme von Daten durch unberechtigte Zugriffe Dritter können nicht ausgeschlossen werden.

- Das MPI-NAT übernimmt keine Verantwortung für die fehlerfreie Funktion der zur Verfügung gestellten Programme. Das MPI haftet nicht für den Inhalt insbesondere für die Richtigkeit, Vollständigkeit und Aktualität der Informationen, zu denen es lediglich den Zugang zur Nutzung vermittelt.
- Im Übrigen haftet das MPI-NAT nur bei Vorsatz und grober Fahrlässigkeit.

Die Nutzungsordnung wird mindestens alle 5 Jahre oder anlassbezogen aktualisiert und im Intranet des Instituts veröffentlicht.

Diese Nutzungsordnung tritt am 1.1.2022 in Kraft.