Richtlinie für das zentrale Mailsystem der Universität Rostock

Inhaltsverzeichnis

1. Allgemeine Hinweise . . . 2
   1.1. Einsatzzweck . . . 2
   1.2. Funktionskonten und vertrauliche Daten . . . 2
   1.3. E-Mailclient und Weiterleitung von E-Mails an Dritte . . . 2
   1.4. Dokumentenaustausch . . . 2
   1.5. Vorgangsbearbeitungssystem (Vertraulichkeit, Verfügbarkeit, Integrität) . . . 3
   1.6. Verschlüsselung von E-Mails (Vertraulichkeit) . . . 3
   1.7. Verfügbarkeit / Sicherstellen des Empfangs einer gesendeten E-Mail . . . 3
   1.8. Signieren von E-Mails (Integrität) . . . 3
   1.9. Versand von E-Mail-Anhängen . . . 3
2. Technische Maßnahmen . . . 4
   2.1. Bedingungen für die Annahme von E-Mails . . . 4
   2.2. Tarpitting . . . 4
   2.3. Greylisting . . . 4
   2.4. Virenscanner und Sandbox . . . 4
   2.5. Spam-Blocker . . . 4
   2.6. Spamfilter . . . 5
   2.7. Nutzerbeschränkungen beim Mailversand . . . 5
3. Organisatorische Maßnahmen . . . 5
   3.1. Maßnahmen im Schadensfall und zur Schadensvorbeugung . . . 5
   3.2. Maßnahmen für den sicheren Betrieb . . . 6
   3.3. Händisches Löschen und Manipulation von E-Mails . . . 6
   3.4. Dateneinsicht generell . . . 6

Dokument

Dieses Dokument ist gültig. Es ist für Nutzende der UR-Nutzerkennzeichen verbindlich.

- Freigabe am: 07.08.2025
- Freigabe durch: Leitung ITMZ

Die Universität Rostock betreibt ein Mailsystem, mit dem die Inhaber von Nutzeraccounts E-Mails empfangen und senden können. Das Mailssystem bietet auch weitere Kollaborationsmöglichkeiten: Kalender, Adressbuch sowie eine Aufgabenverwaltung.

1. Allgemeine Hinweise

1.1. Einsatzzweck

Es wird für Mitarbeitende empfohlen, das Mailsystem ausschließlich für dienstliche Zwecke zu nutzen. Für den Fall der privaten Nutzung wird empfohlen die empfangenen und gesendeten privaten E-Mails in erkennbaren Ordnern von den dienstlichen E-Mails zu trennen. Nur auf diese Weise kann sichergestellt werden, dass es zu keiner Einsicht in private Inhalte kommt, falls es im Ausnahmefall zur Einsicht in die dienstlichen Daten kommt.

1.2. Funktionskonten und vertrauliche Daten

Es ist möglich, für bestimmte Rollen statt mit persönlichen Konten mit Funktionskonten zu arbeiten, die oft auch für mehrere Personen zur Bearbeitung eingebunden werden.

Die meisten Nutzenden gehen davon aus, dass Funktionskonten von mehreren Mitarbeitenden, die persönlichen Konten nur von einem Studierenden/Mitarbeitenden gelesen werden, und E-Mails nicht an Kolleginnen/Kollegen bei Abwesenheit automatisch weitergeleitet werden. Dies ist jedoch nicht sichergestellt für alle Mitarbeitenden und alle Konten. Falls das Mailsystem zum Versenden von vertraulichen Informationen wie Personalsachen und Daten von Studierenden verwendet werden soll, so sind hierfür die Kommunikationsregeln zwischen den Beteiligten abzustimmen.[1]

1.3. E-Mailclient und Weiterleitung von E-Mails an Dritte

- Es wird für Mitarbeitende empfohlen, eingehende E-Mails nicht automatisiert und nur in Ausnahmefällen händisch an ein E-Mailkonto eines Drittanbieters weiterzuleiten, da dies z.B. bei der Übermittlung einer eine andere Person betreffende Personalsache ein der Landesdatenschutzbehörde meldepflichtiger Datenschutzverstoß wäre. Eine Weiterleitung ist per Auswahlregel für nicht-vertrauliche E-Mails (z.B. Firmennewsletter) zulässig.
- Es wird für Mitarbeitende empfohlen, E-Mails nicht mit einem bei einem Cloudanbieter betriebenen E-Mailprogramm abzurufen – damit soll verhindert werden, dass UR Nutzerkennung/Passwort sowie die E-Mailinhalte beim Cloudanbieter gespeichert werden. Dies wäre ein IT-Sicherheitsvorfall und in den meisten Fällen ein meldepflichtiger Datenschutzverstoß. Darunter fallen auch bestimmte Desktop-Clientprogramme, die für ihre Arbeit die Cloudfunktionalität nutzen.[2]

1.4. Dokumentenaustausch

Das Mailssystem ist kein System zum Dokumentenaustausch.[3] Zum *regelmäßigen Dokumentenaustausch* und *Austauschen von großen Dateien* wird stattdessen empfohlen, einen Sync and Share Dienst wie die Unibox zu nutzen (oder SharePoint, ein Projektlaufwerk oder in bestimmten Fällen auch GitLab).

1.5. Vorgangsbearbeitungssystem (Vertraulichkeit, Verfügbarkeit, Integrität)

Das Mailsystem ist kein Vorgangsbearbeitungssystem.[4]

Mailsysteme haben Einschränkungen bei Vertraulichkeit, Verfügbarkeit und Integrität:

- Vertraulichkeit: E-Mails können technisch mitgelesen werden und werden beim Transport zu Empfängern außerhalb der UR von Dritten mitgelesen.
- Verfügbarkeit: E-Mails kommen mit hoher Wahrscheinlichkeit beim Empfänger an, aber technische Probleme und Spam-Filter sorgen für eine gewisse Fehlerquote.
- Integrität: E-Mails können beim Transport durch Dritte, aber auch beim Empfänger (und ebenfalls beim Sender) nachträglich modifiziert werden.

1.6. Verschlüsselung von E-Mails (Vertraulichkeit)

Sofern Vertraulichkeit von E-Mails notwendig ist, wird empfohlen diese E-Mails zu verschlüsseln. Verschlüsselung erfordert jedoch das Handeln von Sender und Empfänger – das ITMZ kann dazu beraten.

1.7. Verfügbarkeit / Sicherstellen des Empfangs einer gesendeten E-Mail

Sofern sichergestellt werden muss, dass eine E-Mail auch beim Empfänger ankam, wird empfohlen, telefonisch dies beim Empfänger abzufragen oder um eine E-Mailbestätigung zu bitten. Die automatischen Lesebestätigungen sind kein zuverlässiges Mittel, dies einzufordern. Dies ist nicht notwendig bei internen E-Mails (bei denen Sender und alle Empfängeradressen zu @uni-rostock.de gehören).

1.8. Signieren von E-Mails (Integrität)

Sofern Integrität von E-Mails notwendig ist, wird empfohlen, diese E-Mails zu signieren – das ITMZ kann dazu beraten.

1.9. Versand von E-Mail-Anhängen

Die maximale Größe von Anhängen beträgt 100 MB. Das regelmäßige Versenden von Anhängen an mehrere Empfänger pro E-Mail ist nicht empfohlen. Das Versenden von Anhängen mit einer Auflösung größer als 300 DPI ist nicht empfohlen. Es wird empfohlen die E-Mails mit großen Anhängen nach Versand und Empfang wieder zu löschen.[5] Es wird darauf hingewiesen, dass viele externe Mailserver nur eine deutlich kleinere E-Mailanhanggröße zulassen (oft im Bereich 10 MB bis 25 MB).

2. Technische Maßnahmen

2.1. Bedingungen für die Annahme von E-Mails

E-Mails werden vom zentralen Mailsystem standardmäßig nur angenommen, wenn folgende Bedingungen erfüllt sind:

- die Empfängeradresse existiert
- die Absenderadresse einer authentifiziert übergebenen E-Mail muss mit der E-Mailadresse des Anmeldenutzerkennzeichens übereinstimmen, um das Fälschen von Absenderadressen zu verhindern
- Absenderadressen anonymer E-Mails dürfen keine Mailadressen des zentralen Mailsystems der Universität Rostock enthalten, um das Fälschen von Absenderadressen einzuschränken
- die Maildomäne der Absenderadresse muss einen gültigen DNS-Eintrag besitzen
- die IP-Adresse des zustellenden Mailclients muss einen gültigen DNS-Eintrag besitzen (Typ A-, CNAME oder MX-Eintrag und dazugehöriger PTR-Eintrag) und darf nicht mehr als 20 gleichzeitige Verbindungen aufgebaut haben
- die HELO/EHLO-Domäne des zustellenden Mailclients darf nicht mit der Domäne der Empfängeradresse übereinstimmen und muss korrekt übergeben werden
- der Spamwahrscheinlichkeitwert (SCL-Wert) muss kleiner als 8 sein

2.2. Tarpitting

Für alle Fehler, die innerhalb der SMTP-Kommunikation durch den zustellenden E-Mailclient erzeugt werden (falsches SMTP-Verb, falscher Empfänger usw.), wird die nächste Reaktion des Mailservers um 5 Sekunden verzögert (Tarpitting).

2.3. Greylisting

Für alle Maildomänen, deren Mailadressen dem Mailserver der Universität Rostock nicht bekannt sind (gehostete Domänen von externen Einrichtungen), ist Greylisting aktiviert.

2.4. Virenscanner und Sandbox

Jede angenommene E-Mail wird auf Viren geprüft. Bei Virenbefall wird sie gesäubert und dem Empfänger zugestellt.

2.5. Spam-Blocker

Der Spam-Blocker ist standardmäßig aktiviert. Alle E-Mails mit einem Spamwahrscheinlichkeitwert (SCL-Wert) 8 oder 9 werden abgewiesen. Alle Nutzenden haben die Möglichkeit, dies über das Webinterface des E-Mailservers der Universität Rostock für seine Mailbox anzupassen.

2.6. Spamfilter

Der Spamfilter ist standardmäßig eingeschaltet. Alle Nutzenden haben die Möglichkeit, dies über das Webinterface des E-Mailservers der Universität Rostock anzupassen.

2.7. Nutzerbeschränkungen beim Mailversand

Das Mailsystem begrenzt die Anzahl der Empfänger einer E-Mail.

Maximale Anzahl der adressierbaren Empfänger pro versendeter E-Mail

```
Studierende: 20
Mitarbeitende: 30
```

Der E-Mailversand ist nicht unbegrenzt möglich. Es wird die Anzahl der Empfänger begrenzt. Es erfolgt eine Sendesperre nach Überschreiten der maximalen Nachrichtenzahl.

Standardeinschränkungen für Nutzer beim Versenden an externe Empfänger

Diese maximale Nachrichtenzahl gilt standardmäßig für Studierende:

```
Nachrichten pro Stunde: 30
Nachrichten pro Tag: 500
```

Diese maximale Nachrichtenzahl gilt standardmäßig für Mitarbeitende:

```
Nachrichten pro Stunde: 210
Nachrichten pro Tag: 5000
```

Falls diese Werte für Ihre Arbeitsweise zu restriktiv sind, senden Sie bitte eine formlose E-Mail an postmaster@uni-rostock.de mit der Bitte, die Werte für Ihr Postfach zu erhöhen.

3. Organisatorische Maßnahmen

3.1. Maßnahmen im Schadensfall und zur Schadensvorbeugung

Im Falle eines Massenversands von E-Mails mit sicherheitstechnisch oder für die Außenwirkung der UR unerwünschtem Inhalt (z.B. Password-Phishing-E-Mails aber auch Werbe-Spam) werden diese E-Mails durch das ITMZ aus den betroffenen Mailboxen des zentralen Mailsystems entfernt. Es wird davon ausgegangen, dass in den meisten Fällen das Nutzerkonto in falsche Hände gefallen ist oder dass Schadsoftware auf einem Gerät des Nutzenden installiert ist. Bei Bedarf wird daher das UR-Nutzerkennzeichen des Verursachers vorsorglich gesperrt, um weiteren Schaden und Identitätsdiebstahl vorzubeugen. Das Nutzerkennzeichen kann meist nach Passwortänderung

und/oder Bereinigung/Neuinstallation der Geräte wieder aktiviert werden.

3.2. Maßnahmen für den sicheren Betrieb

Es erfolgen fortlaufend Maßnahmen zur Absicherung des Betriebs. Aus Sicht des Betreibers ist das Bereitstellen eines abgesicherten Mailsystems höher gewichtet als die Verfügbarkeit – es erfolgen regelmäßig Wartungsfenster und die Sicherheitsmaßnahmen werden angepasst, sodass es z.B. beim Betrieb des SPAM Filters auch zu false positives[6] kommen kann.

Es erfolgt durch das ITMZ die Erhebung von Statistiken u.a. zur Größe von Postfächern sowie Umfang des E-Mailversands und E-Mailempfangs. Die Inhaberinnen und Inhaber der größten Postfächer werden zur Arbeitsweise mit dem Mailsystem beraten.

3.3. Händisches Löschen und Manipulation von E-Mails

Um Schaden von der UR abzuwenden, ist es dem ITMZ möglich und gestattet, einzelne E-Mails zu löschen oder von diesen Anhänge zu entfernen.

3.4. Dateneinsicht generell

Eine Einsicht in Inhalte von E-Mails erfolgt i.d.R. nicht. Die Administratorinnen und Administratoren des Mailsystems sind zur Verschwiegenheit verpflichtet, falls es bei technischen Maßnahmen zur Kenntnisnahme von privaten oder dienstlichen Informationen kommt.

3.4.1. Dateneinsicht aus technischen Gründen

Eine Einsicht durch Mailsystem-Administratoren kann aus technischen Gründen notwendig sein, z.B. wenn im Rahmen der Bearbeitung eines IT-Sicherheitsvorfalls auf Anweisung von IT-Sicherheitsbeauftragtem, ITMZ-Leitung oder zuständiger Abteilungsleitung mit festgelegten Suchmustern nach E-Mails gesucht wird. Eine Einsicht kann in Ausnahmefällen auch für die Durchführung von technischen Administrationsaufgaben notwendig sein. Bei dieser Einsicht ist es, u.a. durch die Wahl der Suchmuster möglichst zu vermeiden, Einblick in die dienstliche oder private Kommunikation zu nehmen.

3.4.2. Dateneinsicht aus organisatorischen Gründen

- Das Mailsystem dient der dienstlichen Kommunikation an der UR und mit externen Partnern. Sofern es dienstlichen Gründen erforderlich ist, dass eine Einsicht in die gesendeten und empfangenen E-Mails zu nehmen ist, dann erfolgt dies unter hoher Sensibilität u.a. mit der Beteiligung der Personalstelle sowie des zuständigen Personalrats. Dies ist ein Ausnahmefall, der aber erfolgen kann z.B. bei kriminellen Handlungen, schwerwiegenden Verstößen oder keiner Möglichkeit, der Dateneinsicht selber einzuwilligen.
- Eine Dateneinsicht aus privaten Gründen durch Bevollmächtigte Dritte ist in Ausnahmefällen in einem ähnlichen Verfahren ebenfalls möglich.

[1] Dies ist nötig, da es keine universitätsweite Regelung gibt und aufgrund der Struktur der Universität keine geben kann.

[2] Dies ist nicht anders möglich, die Weitergabe des Passwortes an andere ist ein Verstoß gegen *§ 5 Rechte und Pflichten der Nutzerinnen/Nutzer* der Nutzungsordnung des ITMZ.

[3] Ein gelegentlicher Austausch von Dateien ist in Ordnung, es sollte aber auf die Größe der Anhänge geachtet werden, und insbesondere sollten größere Dateien nicht dauerhaft im Mailsystem gespeichert bleiben.

[4] Ein Vorgangsbearbeitungssystem ist ein IT-System bei dem meist mit einem Workflow Metadaten und Dateien bearbeitet und schließlich endgültig in einem Dokumentenmanagementsystem abgelegt werden.

[5] Der E-Mailsserver und der eigene E-Mailclient werden langsamer bei sehr vielen oder bei großen E-Mails. Es ist daher besser, die Anhänge im Dateisystem zu speichern.

[6] False positives bei SPAM Filtern sind zu Unrecht als SPAM identifizierte E-Mails. SPAM wird im Wesentlichen aufgrund von statistischen Merkmalen erkannt und so ist es nicht immer technisch möglich z.B. einen Newsletter von Werbespam zu unterscheiden. Daher ist es wichtig im Mailclient regelmäßig neben der eigenen INBOX auch den SPAM-Ordner durchzugehen.