Richtlinie für Studierenden-IT

Inhaltsverzeichnis

Richtlinie . . . 1
- Nutzungsberechtigte . . . 1
- Voraussetzungen . . . 2
- Rahmenbedingungen . . . 2
  - Anbindung ans Identitätsmanagement . . . 2
  - Nutzung von virtuellen Maschinen (VM) und Storage . . . 2
  - Betrieb von Basisnetzwerkdiensten . . . 2
  - IT-Sicherheitsvorfälle . . . 2
  - Datenschutz und Datenschutzvorfälle . . . 3

Hinweise an potenzielle Nutzer:innen . . . 3

Dokument

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

- Freigabe am: 01.08.2025
- Freigabe durch: Leitung ITMZ
- Erstmalige Veröffentlichung am: 01.08.2025

Die Studierendenschaft der Universität Rostock kann IT-Dienste im Netz und mit Ressourcen der Universität anbieten, dies erfordert abweichende Regelungen von den Regelungen, die für Mitarbeitende gelten.

Richtlinie

Nutzungsberechtigte

Virtuelle Maschinen, Storage und andere Dienste des ITMZ können beantragt werden von:

- Einrichtungen der verfassten Studierendenschaft der Universität Rostock
- Hochschulgruppen, die beim AStA der Universität Rostock akkreditiert sind
- Landeskonferenz der Studierendenschaften Mecklenburg-Vorpommern

Die Beantragung für andere Gruppen oder Personen ist nicht möglich. Verantwortlich für den Betrieb ist jeweils die Antragstellerin.

Voraussetzungen

- Die Nutzung von Diensten erfordert eine aktive und vom ITMZ erreichbare technische Administration. Es muss eine Erreichbarkeit sichergestellt werden, ansonsten kann es, analog zum Vorgehen bei allen anderen IT-Systemen der UR, bei Sicherheitsvorfällen zur Sperre und ggf. Abschaltung von Diensten durch das ITMZ kommen.
- Das ITMZ ist nur technischer Betreiber der Infrastruktur. Wer aus der Studierendenschaft einen Dienst anbietet, ist sowohl für die unter eigener Kontrolle liegende Technik (z.B. Administration des Betriebssystems der virtuellen Maschine) als auch vollumfänglich für IT-Sicherheit und Datenschutz verantwortlich. Dies ist bei den Diensten auch jeweils so darzustellen.

Rahmenbedingungen

Anbindung ans Identitätsmanagement

Die Anbindung eines eigenen Dienstes an einen Identityprovider (IdP) des ITMZ kann nur mittels Serviceprovider (SP) erfolgen. Dazu ist ein Antrag zu stellen. Zulässig ist nur eine Nutzung von Shibboleth. Für Bestandssysteme gilt eine Übergangsfrist für die Nutzung von anderen Anbindungstypen (z. B.: LDAP/ADS). Die bisherigen Verfahren (LDAP/ADS) werden innerhalb von 3 Monaten nach erstmaliger Veröffentlichung dieser Richtlinie deaktiviert.

Nutzung von virtuellen Maschinen (VM) und Storage

Es ist möglich virtuelle Maschinen für den Betrieb von Diensten zu beantragen, die zum Speichern Storage und Backupdienst des ITMZ nutzen können. Das ITMZ wird die Inhalte des Storage nicht prüfen (dafür ist der Diensteanbieter verantwortlich). Es ist aber eine Meldung an das ITMZ nötig:

- Welche Dienste werden auf diesen virtuellen Maschinen betrieben (z.B. „Wordpress auf Apache Server“ oder „Nextcloud“)?
- Wer ist Ansprechperson, und wie ist die Ansprechperson erreichbar?

Diese Meldung muss bei Änderungen erneut erfolgen.

Betrieb von Basisnetzwerkdiensten

Ein Betrieb von Diensten welche grundlegende Netzwerkfunktionalität (z.B. DNS) oder Zugang bzw. externe Nutzung des Netzwerks der UR bietet (z.B. VPN/WLAN/Internet Connection Sharing) ist nur in gesonderten Fällen und nach Absprache (Genehmigung und Festlegung der Bedingungen) mit dem ITMZ möglich.

IT-Sicherheitsvorfälle

Bitte melden Sie IT-Sicherheitsvorfälle auch an den Informationssicherheitsbeauftragten der UR: it-sicherheit@uni-rostock.de

Datenschutz und Datenschutzvorfälle

Für Ihre Datenschutzbelange ist die Datenschutzbeauftragte der Studierendenschaft zuständig: datenschutz.asta@uni-rostock.de

Hinweise an potenzielle Nutzer:innen

Der Betrieb von IT-Systemen ist mit Verantwortung und Risiken verbunden. Bitte prüfen Sie, inwieweit Sie dies selber erbringen können. Die Universität stellt Ihnen für Ihre Arbeit auch die vom ITMZ betriebenen Dienste bereit. Diese mögen vielleicht nicht in allen Punkten Ihren Anforderungen entsprechen, decken jedoch einen großen Teil an Kollaborationsanforderungen bereit. Bitte hinterfragen Sie auch im laufenden Betrieb immer wieder kritisch, inwieweit Sie weiterhin selber Dienste anbieten können.

Die Abschaltung von Diensten bei Nichterreichbarkeit erfolgt nach einer angemessenen Frist. „Ich bin gerade im Urlaub und melde mich nach der Rückkehr dazu“ ist bei Sicherheitsvorfällen nicht akzeptabel, während es schon klar ist, dass Sie in den meisten Fällen nicht sofort reagieren können – dies ist bei Beschäftigten ebenso.