Richtlinie zum Umgang mit veralteten Betriebssystemen

Inhaltsverzeichnis

Windows 7 und ältere Versionen . . . 1
Windows 10 . . . 2
Empfohlen: Upgrade . . . 2
Alternative 1: Einkauf von Sicherheitsupdates . . . 2
Alternative 2: Betrieb in abgeschotteten Netzbereichen . . . 2
Alternative 3: Weiterbetrieb ohne etwas zu tun . . . 3
andere Betriebssysteme . . . 3

Dokument

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

- Freigabe am: 07.10.2025
- Freigabe durch: Leitung ITMZ

In dieser Richtlinie wird der Umgang mit veralteten Betriebssystemen auf Endgeräten beschrieben. Endgeräte mit veralteten Betriebssystemen stellen ein erhebliches Sicherheitsrisiko dar, wenn sie im Universitätsnetz verwendet werden. Auch eine Verwendung außerhalb des Universitätsnetzes ist ein Sicherheitsrisiko, wenn vom Gerät aus Dienste der Universität genutzt werden.

Windows 7 und ältere Versionen

Einstellung des Supports

Bereits am 13.01.2015 endete der Support für Windows 7. Gegen jährliche Abogebühr war ein erweiterter Support bis zum 14.01.2020 einkaufbar.

Ein Betrieb von Windows 7 und älteren Versionen ist an der UR nur dann möglich, wenn dies in einem Netzbereich mit kompletter Netztrennung vom Universitätsnetz erfolgt. Geräte mit solch alten Betriebssystemen dürfen nicht (auch nicht kurzzeitig) im Universitätsnetz mit Netzanbindung betrieben werden.

Regelung für Forschungsgeräte

Ein Sonderfall sind Geräte mit Windows 7 (und älter) für den Betrieb von Forschungsgeräten wie z.B. Messgeräten. Das Melden dieser Geräte an den ISB ist erforderlich (per E-Mail an it-sicherheit@uni-rostock.de). ISB und Nutzer:innen erarbeiten gemeinsam eine Lösung. Ohne Bearbeitung und Freigabe durch den ISB

wird das ITMZ den Zugang dieser Geräte in das Universitätsnetz und zum Internet aus Sicherheitsgründen sperren.

Windows 10

Einstellung des Supports

Am 14. Oktober 2025 endet der weltweit verfügbare kostenlose Support für das Betriebssystem Windows 10 (Versionen Home, Pro und Education). Es werden keine Sicherheitsupdates mehr ohne Gegenleistung veröffentlicht. Kostenlose Sicherheitsupdates sind mit einem für die UR nicht akzeptablem Preis verbunden - der dafür nötigen Anbindung an die Cloud.

Empfohlen: Upgrade

Es wird empfohlen, entweder ein Upgrade/Neuinstallation auf Windows 11 oder auf ein alternatives supportetes Betriebssystem (z.B. eine aktuelle Linux Distribution) durchzuführen. Mit Windows 11 wurden die Hardwareanforderungen erhöht. Falls ein Upgrade neue Hardware erfordert, ist der Austausch der Hardware auch bei kurzer Nutzungsdauer begründbar, sofern kein alternatives Betriebssystem genutzt werden kann.

Alternative 1: Einkauf von Sicherheitsupdates

Es können für einen begrenzten Zeitraum Sicherheitsupdates für Windows 10 eingekauft werden. Der Einkauf ist für die EDU-Lizenzen der UR möglich, die Kosten werden deutlich unten den öffentlich von Microsoft genannten Preisen für Privatnutzer. Die jährlichen Kosten steigen pro Jahr deutlich. Der Einkauf der Updates zum vollen Preis ist monetär nicht wirtschaftlich gegenüber dem Neukauf von Windows 11 und bietet nur einen geringen Aufschub für das unumgängliche Upgrade. Dies sollte daher nur erfolgen, wenn es aus anderen Gründen eine wirtschaftliche Lösung ist. Die Entscheidung sollte begründet werden.

Alternative 2: Betrieb in abgeschotteten Netzbereichen

Zusammen mit der Netzwerkabteilung des ITMZ kann die Netzstruktur so angepasst werden, dass die Gefährdung des Universitätsnetzes durch die Geräte stark verringert wird.

Regelung für Forschungsgeräte

Ein Sonderfall sind Geräte mt Windows 10 für den Betrieb von Forschungsgeräten wie z.B. Messgeräten. Das Melden dieser Geräte an den ISB ist erforderlich (per E-Mail an it-sicherheit@uni-rostock.de). ISB und Nutzer:innen erarbeiten gemeinsam eine Lösung.

Alternative 3: Weiterbetrieb ohne etwas zu tun

Das ITMZ behält sich vor, Windows-10-Rechnern, ab dem den Zeitpunkt des Supportendes aus Sicherheitsgründen den Zugang in das Universitätsnetz und zum Internet zu sperren.

andere Betriebssysteme

Auch für andere veraltete Betriebssysteme besteht die Empfehlung, ein Upgrade auf ein supportetes Betriebssystem durchzuführen. Das ITMZ behält sich vor, den betroffenen Rechnern aus Sicherheitsgründen den Zugang in das Universitätsnetz und zum Internet zu sperren.