



E-Mail Mail Policy

In diesem Dokument wird der derzeitige Stand der Policy (Regelwerk zur Behandlung von E-Mails) des Mailservers der Universität Bielefeld beschrieben.

- > Die Maileingangsrelays basieren auf den SOPHOS Produkt [PureMessage](#).
- > Alle anderen Komponenten werden durch das SUN Java Enterprise System realisiert.
- > Bei der **Etablierung von neuen Mailservern/Domänen** innerhalb der Universität/FH muss das HRZ kontaktiert werden, um die notwendigen MX Records im DNS zu etablieren und das Mailrouting einzurichten.
- > Die **Gültigkeit von Mailadressen** wird mit dem "call-forward" Verfahren überprüft. Beim Einliefern der Mail auf dem Gateway wird per SMTP Dialog auf dem Zielsystem die Mailadresse überprüft. Ist diese bekannt, wird die Mail angenommen und zugestellt. Andernfalls wird die Annahme abgelehnt (500er Returncode). Im Störfall erhält der einliefernde Server einen temporären Zustellungsfehler (400er Returncode).
- > Behandlung von **Viren**: Die Gateways scannen die Mails beim Einliefern auf bekannte Viren. Bei Mails, die Viren enthalten, wird die Annahme abgelehnt (500er Returncode). Ansonsten erfolgt die weitere Verarbeitung.
- > Behandlung von **SPAM**: Die Gateways bewerten Mails beim Einliefern und unterscheiden in 3 Fälle:
 - > **Spambewertung >= 80%**: Die Annahme der Mail wird verweigert (500er Returncode).
 - > **Spambewertung 50% bis 79%**: Die Mail wird angenommen und in der Quarantäne zurückgehalten. Der Nutzer erhält 1-mal am Tag (Nachmittag) eine Zusammenfassung (Digest) seiner Mails, sofern E-Mails in der Quarantäne vorhanden sind. Diese Mails kann man sich per "Click" zustellen lassen. Die Mails werden **40 Tage** in der Quarantäne aufbewahrt.
 - > **Spambewertung < 50%**: Die Mail wird zugestellt.
- > **Betreiber eigener Mailsdienste** bekommen alle SPAM-Mails zugestellt. Es erfolgt die Markierung im Header und der Subject Zeile bei >50% Spambewertung: Am Anfang der **Subject/Betreff** Zeile wird **[SPAM]** eingefügt. Diese Informationen können zur Formulierung von Filterregeln in den Mailclients herangezogen werden.
- > Das Verhalten, wie Viren und SPAM behandelt werden kann jeder Nutzer des HRZ/FH Mailsdienstes für seine Mailadressen in der [BenVW](#) ändern.
- > Limitierung der IP Verbindungen pro Zeiteinheit für Rechner im Internet. Beim Überschreiten eines Schwellwertes: Temporärer Zustellungsfehler (400er Returncode).
- > Limitierung der Anzahl E-Mails pro Zeiteinheit und sender E-Mail Klienten/Server. Es sind unterschiedliche Raten für das Intranet und das Internet konfiguriert.
-> Überschreiten: Temporärer Zustellungsfehler (400er Returncode).
- > **RBL (Realtime Blackhole List) Listen**:
 - > RBL Listen werden zur Spambewertung genutzt.
 - > Eine von Sophos gepflegte sehr zuverlässige Liste von IP Adressen wird genutzt, um Mails von diesen Absendern abzulehnen.

- > **Blocken** von bekannten, von Viren statisch genutzten **Absender/Zieladressen**, wie z.B. admin@duma.gov.ru durch den den W32/Dumaru-A Virus, wenn dies sinnvoll erscheint.
- > Um Probleme mit der **Quotierung des Speicherplatzes** zu verhindern, wenn man Mails löscht und damit in den Trash-Folder verschiebt, werden diese nach **40 Tagen** dort automatisch gelöscht. (aktiv ab dem 13.2.2006)
- > **UMS** (Fax + AB Integration): Fax- und Voice-Mails in dem bereitgestellten Shared-Folder (umsadm/<Kennung>) werden nach **270 Tagen** gelöscht.
- > Der Versand von E-Mails über das universitätseigene Mailsystem ist auf eine Menge von **200 Stück** pro Tag und **75 Empfänger** pro E-Mail limitiert. (aktiv ab dem 31. Januar 2011)