

## Retention Policies Page

<https://campus.barracuda.com/doc/51189905/>

### Important

Before defining data retention policies, make sure you have a clear understanding of data and email message compliance rules as well as your organization's record retention policies.

Use retention policies to define the length of time you retain historic data based on daily, forever, or never.

### Important

Purging applies to *historic file revisions only*; your current data is never impacted by a retention policy.

Configure retention policies for data stored in Barracuda Cloud-to-Cloud Backup on the **Backup > Retention Policies** page. Be sure to configure retention policies for your data. Not doing so means that some unwanted data will be moved across the Internet and stored.

## How it Works

Historic data is retained according to the retention policy timeline. Data backed up using Barracuda Networks' cloud treats Sunday as the end of week in accordance with the ISO date standard.

When you define a retention policy, begin by selecting either a preset template or a previously defined policy as a starting point. This helps you avoid creating multiple retention policies for the same sets of data. You can create one policy for all of the data sources in Barracuda Cloud-to-Cloud Backup, or create different policies that include subsets of the data.

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.