AvePoint Cloud Backup

Essential Eight Regular Backups Requirements vs. AvePoint Cloud Backup

The Australian Cyber Security Centre advocates having regular backups as one of the three most vital aspects of the Essential Eight to protect your organisation against cyber threats.

Here's a summary of Essential Eight's Maturity Level 3 requirements and how AvePoint delivers compliant regular backups for customers.

Essential Eight Regular Backup Maturity Level 3 Requirements	How AvePoint Delivers Essential Eight Regular Backups Maturity Level 3 Compliance
1 Backups of important data, software, and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements.	• *AvePoint backs up the broadest range of data, software, and configuration settings available in the Microsoft cloud ecosystem (M365, Azure, Dynamics)* **of any 3rd party data protection vendor.** • *Additionally, our scope continues to grow deeper as Microsoft releases new functionality and supported APIs. This includes not only specific item level data, such as Teams chats and Planner items, but also granular configurations settings such as SharePoint Online site administration, Teams channel and even Power Platform environments.*
2 Backups of important data, software and configuration settings are synchronised to enable restoration to a common point in time.	• *AvePoint backs up customer data up to 4 times per day and retains backups for an unlimited time period.* • *All backup data, software and configuration are synchronised so that restores can be performed at any previous restore point. Our Restore UI is easy to use and available from any device through our AvePoint Online Services portal anywhere in the world.* • *If you elect to store your data in our Microsoft Azure-backed cloud, your restores are also cloud-to-cloud, delivering the most efficient performance available from 3rd party data protection vendors.*
3 Backups of important data, software and configuration settings are retained in a secure and resilient manner.	• *AvePoint's Cloud Backup storage is hosted in one of 14 Azure Data Centres worldwide. In Australia, AvePoint Online Services is hosted in the Australia South East region.* • *Our company processes, services, and software have obtained industry-leading security, privacy, and accessibility certifications. This includes ISO 27001, SOC II and IRAP "Protected" level compliance.* • *Australian Federal government agencies and global financial services organisations trust AvePoint with their data and have validated our process, services and software to be industry-leading.*

4	Restoration of important data, software and configuration settings from backups to a common point in time is tested as part of disaster recovery exercises.	• *Data restoration from AvePoint's Cloud Backup can be tested as part of any disaster recovery exercise 365 days a week, 24/7. We support the restoration of data, software and configuration settings in place or out of place.* • *Additionally, your backup data can be exported for offline consumption, unlocked with a decryption key provided by our Cloud Backup solution.*
5	Unprivileged accounts cannot access backups belonging to other accounts, nor their own accounts.	• *Cloud Backup includes delegated administration and role-based access controls to ensure that unprivileged accounts do not have access to backups belonging to either their own accounts or to other accounts.*
6	Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts, nor their own accounts.	• *Cloud Backup includes both delegated administration controls and the ability to create flexible containers to group workloads and user accounts together. Using both delegated administration and containers, privileged accounts (excluding backup administrator accounts) do not have access to backups belonging to either their own accounts or to other accounts.*
7	Unprivileged accounts are prevented from modifying and deleting backups.	• *Cloud Backup includes delegated administration and role-based access controls to ensure that unprivileged users are prevented from modifying and deleting backups. Unprivileged accounts will not have access to Cloud Backup to be able to modify or delete backups.*
8	Privileged accounts (including backup administrator accounts) are prevented from modifying and deleting backups during their retention period.	• *The ability for privileged accounts (including backup administrator accounts) to modify or delete backups can be disabled, making backups immutable until they reach their retention period set within Cloud Backup.* • *The retention period for backups can be set at both a workload and a detailed container level to enable for granular control over the retention of backups.* • *A customer can only enable manual deletion of backup data through direct contact with AvePoint Support (included with Cloud Backup) and provide verification to proceed with deletion.*

Get Essential Eight Compliant Today!

At AvePoint, our Cloud Backup solutions are built to protect your data. As a global business, our platform is designed to deliver against local Australian and global security standards, including the Essential Eight.

Reach out to our security experts today to find out how you can mitigate today's ever-increasing security risks.