**SECURE COMPLETE CONTROL AND PROTECTION
FOR MICROSOFT 365 DATA:**

The Checklist for Government Agencies

The top misconception about Microsoft 365 (M365) is who is responsible for what. Put simply: Microsoft takes care of the infrastructure, but the data remains the customer's responsibility. Data backup and recovery is therefore also your responsibility.

With that out of the way, we've pulled together a checklist specifically for Government agencies of factors to consider as you plan your Microsoft 365 roll-out.

✓ Are you confident your data retention compliance obligations will be met?

Government agencies have a legal obligation to retain information relating to their business. This applies to a broad range of documents and written communications. When you migrate to M365, you need to be certain you will meet these compliance requirements. Ensuring you have a backup solution that protects you from loss, disruption and corruption of data is critical to avoid breach of your data retention obligations.

✓ Does your implementation of M365 meet your security compliance obligations?

Government agencies are bound by a range of security requirements, designed to protect the data of Australian citizens. Compliance should be a minimum standard — a base layer that you build on to ensure robust and reliable security that goes over and above the bare minimum. How mature is your planned M365 security – especially when it comes to secure and reliable backup of your data? Do you have a process to recover data in the instance of accidental deletion?

When a user is deleted from M365, this also initiates a replicated deletion of the personal SharePoint site

and OneDrive data across the network. If an accidental hard deletion takes place, only some data may be recoverable using M365 native functionality. The process you have in place to recover data in this instance is critical to avoid loss of data and disruption of business continuity.

✓ Have you updated your external security protocols and training for users on your M365 instance?

The cyber-threat environment is increasingly challenging. A move to a new platform with the possibility of access from new endpoints, requires teams to refresh their cybersecurity awareness - appropriate training is therefore a MUST. The limited backup and recovery functions in Exchange Online mean that in the event of an incident not all data may be recoverable. This is why a reliable backup of M365 is imperative.

✓ Have you chosen a hybrid M365 deployment?

Maintaining both cloud and on-premise Exchange deployments is a common strategy to add flexibility and control. If this strategy is adopted, a backup solution designed to adequately cater for this configuration is also required. To optimize

1800-AUCLOUD (1800 282 5683)
sales@australiacloud.com.au
australiacloud.com.au

Assuring Sovereign Resilience

your strategy, you need to ensure nothing 'falls through the gaps' - both from a security and data retention perspective.

✓ Is a "point in time" mailbox restoration capability required by your Data Retention policy?

Point in Time restoration of a user mailbox – for instance to rollback to a particular time before an incident – is not supported within the Microsoft backup and retention capabilities for M365. You will need to ensure your backup solution addresses these retention policy gaps.

✓ Is your Microsoft 365 data backed up to an Australian sovereign location, for both on-premise and cloud?

Backup needs to be dynamic. Government agencies need to be able to back up Microsoft 365 data and applications (whether on premise or in a cloud), to a location of their choosing. Given the confidential nature of most Government data, this should be in a 'sovereign' location. In the case of cloud, knowing where your data resides and who has access to it, is imperative. Only a sovereign cloud provider can guarantee that your data remains in Australia – always.

If this checklist got you thinking about how you have implemented or plan to implement your Microsoft 365 rollout you're not alone. Importantly, it is not too late to ensure you have all your bases covered.

As a cloud IaaS provider exclusively focused on servicing the high security and compliance needs of Government, AUCloud is specialized in delivering solutions purpose-built to meet Government requirements. Our backup and recovery solutions are specifically designed to protect your critical data, enhance your compliance and ensure your agency meets best data management and protection practice.

NEXT STEPS   **THE TEAM AT AUCLOUD - Australia's sovereign cloud Infrastructure-as-a-Service (IaaS) provider - is available now to assist you as you plan your deployment.**

Please contact our sales team at: **1800 282 5683**