



Office of Information Technology Services Policy	No: ITS-P21-005
ITS Policy: Deprovisioning of M365 Accounts and Home Drive(s)	Issued: 05/21/2025
	Issued By: NYS Office of Information Technology Services Owner: Division of Legal Affairs

1.0 Purpose and Benefits

The Office of Information Technology Services (ITS) is entrusted with managing the data of ITS supported agencies. Part of managing this data means maintaining a standardized process for proper data sanitization of accounts and home drive data upon State employee, contractor, or consultant separation. This policy establishes a collaborative workflow that involves ITS technical staff, ITS Division of Legal Technology (herein after referred to as “DLT”), and Client Agency legal counsel, or their designee.

2.0 Authority

Section 103(10) of the State Technology Law provides ITS with the authority to establish statewide technology policies, including technology and security standards. *Section 2 of Executive Order No. 117¹*, issued January 2002, provides the State Chief Information Officer with the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy, [NYS-P08-002 Authority to Establish State Enterprise Information Technology \(IT\) Policy, Standards and Guidelines](#).

¹ All references to Executive Order 117 refer to that which was originally issued by Governor George E. Pataki on January 28, 2002 and continued by Executive Order 5 issued by Governor Eliot Spitzer on January 1, 2007, Executive Order 9 issued by Governor David A. Patterson on June 18, 2008, Executive Order 2 issued by Governor Andrew M. Cuomo on January 1, 2011, and Executive Order 6 issued by Governor Kathy Hochul on October 8, 2021.

3.0 Scope

This policy applies to ITS, its employees, contractors, consultants, and ITS supported agencies (“Client Agency”).

This policy applies to data repositories assigned to a specific user.

4.0 Information Statement

ITS DLT is a Division within the Office of the Chief General Counsel. DLT provides legal preservation services to ITS and Client Agencies for both email and non-email electronically stored information (ESI). To assist ITS and Client Agencies in meeting their legal preservation obligations, including those associated with investigations, litigation, administrative matters, and statutory requirements, DLT has established legally defensible protocols around data collection, preservation, transfer, and destruction. To ensure ITS and Client Agencies can meet their legal obligations on this topic, it is imperative that all ITS business units consult with DLT as outlined in this policy.

4.1 Microsoft 365 (M365) Deprovisioning upon Employee, Contractor, or Consultant Separation

This policy is intended to supplement the Inactive Mailbox Management Process, dated May 2016 and as amended April 2020, attached in Section 9 of this document.

After a state employee, contractor, or consultant leaves state service or transfers to another state agency, the user’s M365 account will automatically begin the deprovisioning process and will be purged within 60 days of the separation date. This process will also automatically remove the user’s email address from all associated distribution groups and the statewide Global Address List (GAL).

The deprovisioning process described above does not apply to email or other account data that has been placed on a legal hold by a Client Agency’s legal counsel, or their designee, through use of the electronic preservation mechanisms available through the ITS-managed M365 system. If a Client Agency’s legal counsel encounters issues with placing a legal hold on a user’s mailbox or other account data, a request for support must be sent to the ITS DLT at its.sm.legaltech@its.ny.gov.

4.2 Home Drive Destruction upon Employee Separation

After a state employee, contractor, or consultant leaves state service or transfers to another state agency, the user’s home drive data will be purged one (1) year from the separation date.

Should a user’s home drive data be required for either business continuity or legal preservation, the requesting Client Agency’s legal counsel, or their designee, must send a formal request to DLT at its.sm.legaltech@its.ny.gov. Material placed on a legal hold is retained until such time as the Client Agency’s legal counsel, or their designee, purges the preserved data.

5.0 Compliance

This policy shall take effect upon publication. Compliance is required with all ITS policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is required.

6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in <http://www.its.ny.gov/glossary>.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Division of Legal Technology
Reference: ITS-P21-005
NYS Office of Information Technology Services
State Capitol, ESP, P.O. Box 2062
Albany, NY 12220
Telephone: 518-473-5115
Email: its.sm.legaltech@its.ny.gov

ITS policies, standards, and guidelines may be found on the ITS website at:
<https://its.ny.gov/policies>

8.0 Revision History

This policy should be reviewed consistent with the requirements set forth in [ITS-P24-003 Process for Establishing Information Technology Polices, Standards and Guidelines](#).

Date	Description of Change	Reviewer
09/03/2021	Issued policy	Division of Legal Affairs
05/21/2025	Changed owner to DLT; expanded policy to M365 accounts	Chief General Counsel

9.0 Related Documents

**OFFICE 365 INACTIVE ACCOUNT MANAGEMENT
PROCESS EFFECTIVE MAY 2016
AMENDED APRIL 3, 2020,
MODIFIED MAY, 21, 2025**

This document describes the process for agency and ITS management of Microsoft 365 accounts (the “May 2016 Inactive Mailbox Management Process”). The May 2016 Inactive Mailbox Management Process became effective in May 2016 and updated certain key features of the inactive mailbox management process previously issued in January 2015.

The following chart contains a high-level description of the how the May 2016 Inactive Mailbox Management Process works with respect to M365 accounts that are inactive after 30 days. The MM, DD, 2024 modification changes this policy from inactive mailbox to inactive account

30 DAYS:	60 DAYS:	90 DAYS:
<p>NO MICROSOFT 365 ACTIVITY</p> <ul style="list-style-type: none"> *account appears on stale report sent to agency shared mailbox *account still receives mail *owner/named user can login to remove from stale status *agency can submit ticket to indicate leave of absence to remove from stale status (through day 59) 	<p>NO MICROSOFT 365 ACTIVITY</p> <ul style="list-style-type: none"> *account remains on stale report *account is removed from the Global Address List/does not receive mail 	<p>NO MICROSOFT 365 ACTIVITY</p> <ul style="list-style-type: none"> *account is deleted *account and data are not recoverable *keeping an account after 90 days of no outgoing mail activity by owner requires prior notice to ITS; you will be billed retail rates to keep the account

**The process described above does not apply to content in a mailbox that has been placed on a legal hold by agency counsel. Legal holds are placed by agency counsel when counsel identifies email or other account content that must be preserved for legal purposes. Material placed on a legal hold is retained until such time as the agency’s counsel determines it is no longer legally necessary to retain it and releases the legal hold.

ITS Reports to Agency Designees

Consistent with the pre-existing process that commenced in January 2015 and has operated continuously since then, ITS will continue to generate and provide regular reports identifying inactive accounts for agency review. Consistent with the pre-existing process, agencies continue to be required to designate staff to monitor a shared mailbox for purposes of receiving

bi-weekly reports of accounts that have become stale.² Most agencies have already designated staff for this purpose pursuant to the pre-existing process, and these staff continue to have access to the appropriate shared mailbox to ensure compliance with the May 2016 Inactive Mailbox Management Process. If you wish to add a designee, or make changes your agency's designee(s), please notify ITS at its.sm.legaltech@its.ny.gov.

How the standard process for de-activating inactive M365 accounts will work

The May 2016 Inactive Account Management Process is triggered when *the owner (named user) of a M365 account has not signed in to the account* for 30 days.

A report listing these accounts is generated twice each month and sent to the agency's shared mailbox described above so that accounts can be reviewed by the agency designee(s) and be placed on legal hold, or otherwise maintained, if necessary.

For 30 days, the user will continue to have access to the account, it will continue to function, and email and other account content will continue to be retained pursuant to any retention rules that are set within Office365. *If a user logs into this account within these 30 days, the account is no longer stale, and the account will be removed from the report and will not be scheduled for deletion.* This 30-day period gives the agency sufficient time to make sure that, where necessary, the account and its contents are maintained. For example, a user may be out on extended medical or other authorized leave, which explains why they have not accessed their account for 30 days. If a user is on such a leave, the agency should enter a ticket in ITSM indicating a leave start and end date, and ITS will take an action to identify that the account is not considered stale during that identified time period.

If no action is taken to identify the account is not stale, on day 60, the account will be removed from the Global Address list, will no longer receive mail, and all the contents of the mailbox will be scheduled to be emptied on day 90, with the following exception: if the content within any mailbox is placed on legal hold by the agency prior to account de-activation on day 60, the email and other account content will remain intact and accessible through the M365 eDiscovery Center. Agencies will need to use the Office365 eDiscovery features to place a legal hold on any such accounts. Accounts that remain stale through day 90 will be emptied and the license recovered. Data from an emptied mailbox that was not placed on legal hold using the M365 eDiscovery features while the account was active cannot be recovered at this point.

Reviewing reports

Accounts are identified for de-activation either at the request of agency Human Resources/Personnel Office pursuant to the agency's standard separation process management, or because the named user has not logged into the account for at least 30 days. Both of these types of accounts will be listed in reports regularly sent to your agency's shared mailbox for which your agency has designated staff to review. By regularly issuing these reports to agencies, agency program areas and agency General Counsels can validate that there are no programmatic, business or legal reasons to maintain the account or preserve its

² Please note that agencies will continue to receive reports of employees and consultants that ITS has been notified are separating, along with the date such accounts are scheduled to be deleted.

contents, including compliance with records retention requirements. The agency may take action to preserve an account that appears on its stale account reports, or the contents of an account appearing on such reports, by taking the steps outlined in this Inactive Account Management Process.