This agreement is based upon a mutual understanding between ITD and the IT Coordinators Council (reviewed March 8, 2017). In conjunction with ITD's Hosting Service Level Agreement, it acts as a Service Level Agreement between ITD and all customers utilizing the Microsoft Active Directory service.

- ITD shall provide the necessary Domain Controllers and Global Catalog Servers for Active Directory
- ITD is responsible for Enterprise and Domain Administration. This role has full administrative rights to all computers within the Active Directory Forest.
- The ITD Service Desk has enterprise access to Unlock/Reset and Enable/Disable accounts. The ITD Service Desk will only Enable accounts with permission and verification from a Lead Request Manager within the user's agency.
- ITD initially creates an Organizational Unit (OU) and OU Administrator for each agency, along with the first user, computer, and group. This first group (called *agencyname*-ou-admins) is delegated full control over the OU. Administration of the OU then becomes the agency's responsibility, and ownership of the OU and its Group Policy is given to the Agency Administrator group.
- AD group names must start with a 3-letter agency-specific prefix (for example, ITD-ALLUSERS)
- AD computer names must start with a 3-letter agency-specific prefix (for example, ITDPC1)
- AD Description fields must begin with a 4-digit department number (for example, 1120)
- In the AD Attribute Editor, agencies must set "extensionAttribute1" to an upper-case X if they wish to conceal an entry from the Contact a State Employee application on the ND.gov portal
- ITD and agencies shall administer Active Directory in accordance with the EA Access Control Standard
- Active Directory and the data it contains shall not be leveraged in ways that create shadow systems (alternative solutions) to the State's implementation of PeopleSoft/Oracle without prior approval from OMB
- AD User-IDs are synchronized with Microsoft Azure Active Directory

Modifications

Date	SLA Modification
2017-03-08	Added that AD User-IDs are synchronized with Azure AD
2016-12-14	Reiterated that Active Directory data should not be leveraged in ways that create shadow systems to PeopleSoft
2016-09-07	Addressed concealing AD entries from the Contact a State Employee application
2016-03-09	Initial adoption of SLA