Policy & Standard Background

|  |
| --- |
| Name: Standard 182.20.10 – Email Address Naming Standards |
| * Purpose of Action: This standard combines the current email naming standard and guideline to promote standardization across the state . Specifically this standard establishes common E-mail address naming conventions for employee E-mail aliases including the Session Initiation Protocol (SIP) and the User Principle Name (UPN), and the Simple Mail Transfer Protocol (SMTP).  . |
| What is the business case for the policy/standard? |
| This standard designates the state's Email address naming conventions as common solutions for state government to promote common IT practices and provide an integrated end-user experience. This updated is needed as the state transitions from on premises email and other services to M365. This update considers equity concerns that have been identified by agencies and the State’s DEI group. |
| What are the key objectives of the policy/standard? |
| 1. This standard establishes common E-mail address naming conventions for employee E-mail aliases including the Session Initiation Protocol (SIP) and the User Principal Name (UPN), and the Simple Mail Transfer Protocol (SMTP). 2. Combines the current email naming standard and guidelines into one document to establish clear objectives and intended outcomes. 3. Email addresses must be unique in each agency 4. What and who is in scope and out of scope of this standard. 5. Sets a date of 4/1/2022 for agencies to submit a waiver if they are not currently in compliance and what the expected timeline and effort is needed to come in compliance. |
| How does policy/standard promote or support alignment with strategies? |
| This standard supports and promotes alignment with the state’s strategies for:   * Adopting cloud solutions and migrating existing systems to cloud services. * Adopting shared services for common business solutions. * Reducing unnecessary operational complexities and costs. * Modernizing IT infrastructure to promote business innovation. * Protecting the state’s IT assets by improving security and resilience of IT systems. * Advancing efficient and accountable government. |
| What are the implementation considerations? |
| * The policy memorializes what has been statewide practice for several years. Most of the requirements in this standard are in the current OCIO Email naming standard and guidelines or standards approved by the statewide Enterprise Active Directory Steering committee. It combines many of these standards into one standard. * Agencies are in varying degrees of compliance with the current standard as well as this draft standard. * Some agencies may not be able to prioritize resources or have the funding needed to meet the required timeline. They can apply for a waiver, but that means there could be technical and collaboration issues are the State continues to move to cloud based solutions. For some of the agencies not currently in compliance it could mean a major project to transition their legacy naming practices to the ones proscribed in this updated standard. The amount of time and money needed to complete this transition will vary by agency. These agencies can submit a waiver that describes their current state of compliance and the plan moving forward. * This is one of many policy, standards, and guidelines that are needed for efficient and effective adoption of shared cloud resources such as M365. |
| How will we know if the policy is successful? |
| The Policy is successful if all in scope agencies have met the conditions outlined in this standard or have a plan to become compliant. |