State of California

Department of Technology

Workgroup Collaboration Platform Guidelines

SIMM Section 130

January 2020

REVISION HISTORY

REVISION	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Release	JAN 2020	CDT Office of Government Affairs	

Table of Contents

Workgroup Collaboration Platform Guidelines

1.0 Overview

The increased utilization of collaborative tools that emphasize and enable teamwork continues to improve the way government communicates and collaborates. Unified communications platforms promote capabilities that allow remote collaboration. These platforms combine collaboration tools into a single enterprise platform enabling the rapid provisioning of shared workspaces and facilitating distribution of topic-based information. Workgroup Collaboration Platform is defined in State Administrative Manual (SAM) Section 4819.2 as:

> *"Cloud-based collaboration tool that integrates features such as chat, conferencing, calendaring, notes, and attachments organized by topics and accessible through a specific URL or invitation. Within the platform, members can create channels or topics of conversation and collaborate through a shared workspace."*

These guidelines are intended to assist agencies/state entities to develop internal policies and procedures to ensure proper use of workgroup collaboration platforms in accordance with SAM Section 5170. The Workgroup Collaboration Platform policy requires:

> *"Each agency/state entity shall develop and implement policies and procedures to ensure proper use of Workgroup Collaboration Platforms, as defined in SAM Section 4819.2. These policies and procedures must comply with SAM Section 4846 and 5300, which provide that all computer software purchased with state funds is procured in accordance with state law and used in compliance with licenses, contract terms and applicable copyright laws. In addition, management should ensure all staff understand and adhere to proper software management policies that address, at a minimum, the following key areas: acceptable use, public records act considerations, key roles and responsibilities, security/privacy, workspaces and records retention and management of Workgroup Collaboration Platforms."*

The following sections provide guidance for each key area that should be addressed through the creation of an internal agency/state entity policy. This is not an exhaustive list of the areas that should be addressed. Each agency/state entity should carefully evaluate its own practices, procedures and needs to add other relevant areas to its policy.

2.0 Key Roles and Responsibilities

Agencies/state entities should clearly define and assign key roles and responsibilities to effectively manage and maintain the Workgroup Collaboration Platform. Roles and Responsibilities shall designate the following (this is not an exhaustive list):

- Employees authorized to officially procure Workgroup Collaboration Platforms on behalf of the agency/state entity.
- Employees responsible for ensuring contract terms are acceptable to the State.
- Employees responsible for ensuring compliance with security requirements.
- Employees designated as an administrator (more than one person shall be designated for each workspace).
- Employees designated as owners and have the ability to add, invite, and approve members and requests for new workspaces and channels.
- Employees responsible for responding to PRA requests and for appropriately preserving and archiving records consistent with record retention schedules.

3.0 Acceptable Use

An acceptable use policy is required for all employees who access and use state information assets. A set of guidelines should be adopted that describe the proper use of the Workgroup Collaboration Platform, including expectations for utilizing the platform, in order to reduce potential risk to the agency/state entity. It is often common practice to ask new owners, users or members to sign an acceptable use policy before they are given access. For this reason, an acceptable use policy must be concise and clear, while at the same time covering the most important points about what users are, and are not, allowed to do with the platform (e.g. user conduct, security responsibilities, incident reporting, etc.). It should also define what sanctions will be applied if a user breaks the agency/state entity's acceptable use policy and refer users to more comprehensive policy information where relevant. Sample policy language is available at the SANS Institute https://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy.

4.0 Public Records Act (PRA) Considerations

The California Public Records Act (Government Code §§ 6250 through 6276.48) requires inspection or disclosure of governmental records to the public upon request, unless exempted by law. The PRA is intended to safeguard the accountability of government by promoting public disclosure of governmental operations. Workgroup Collaboration Platform communications may be records subject to the PRA. Thus, Agencies/state entities should treat these tools as a public forum. Users should assume everything that is shared will be made public, including file uploads, direct messages, and any audio or video transmitted.

5.0 Security/Privacy

Agencies/state entities should establish minimum requirements for ensuring the configuration, use and maintenance of a Workgroup Collaboration Platform is secure and protects users and data. Security guidelines must include such requirements as two-factor authentication (2FA) and utilize privacy settings. Collaboration tools offer private and public settings and Agencies/state entities should utilize the private setting.

Agencies/state entities should further ensure security by informing users not to post anything that would make systems vulnerable or would impact the privacy of others if it were shared accidentally. Additionally, users should be made aware of privacy consideration such as informing them that public channels can be made accessible to anyone. Users must be aware of any sensitive and confidential data types they are using to collaborate and must take action to minimize accessibility on a need to know basis.

In accordance with SAM Sections 5300, 5305, 5305.4 and National Institute of Standards and Technology (NIST) 500-53 PL-4, each agency/state entity shall ensure personnel are aware of, have agreed to comply with, and understand the consequences of failure to comply with information security policies and procedures. In addition, all personnel must sign an acknowledgement of their security and privacy responsibilities. Non-compliance with security and privacy responsibilities may result in corrective action, including but not limited to, termination.

6.0 Workspaces

Workspaces, also referred to as channels, are created within the Workgroup Collaboration Platform to foster collaboration and communication. Workspaces may be created and operated by an agency/state entity, other government entities, and entities under contract by the state entity or external partners. Agencies/state entity policies should provide guidelines to users on how and when they can create or join workspaces and how they should conduct themselves as members. Guidance should include direction on when users should use either their work email address or personal email address and how invitations to join workspaces should be handled. Guidelines shall also address protocols required for workspaces that are open to the public, considerations may include securing appropriate consent to publish information, acceptable use related to the public, and identification of who may represent the agency/state entity when responding to public feedback.

7.0 Records Retention and Management

In accordance with SAM Section 1611, each agency/state entity must establish a Records Retention Schedule program consistent with state and agency statutory requirements. Agencies/state entities shall update their Records Retention Schedule to ensure that all records produced, maintained, or disposed of through an agency/state entity's Workgroup Collaboration Platform are properly and timely retained. Certain Workgroup Collaboration Platforms may allow the user access to set the retention policy of their workspace. If this is an option, the owner of the workspace must set the retention in accordance with the agency/state entity's Records Management Program. Communications that constitute "records" must be retained consistent with the agency/state entity's Records Retention Schedules either in the workspace or exported to an external archive location. Users are responsible for retaining all communication history based on the agency/state entity's Records Retention Schedule. It is recommended that agencies/state entities do not use the auto delete option.