LACCD Office 365 Collaboration Protocol and Procedures: MS Teams and SharePoint

Version Control				
#	**Date**	**Editor**	**Approved**	**Changes**
0.8	09/09/2020	C. Nersisyan		Initial Document
0.9	09/10/2020	C. Nersisyan		Group Edits
0.91	9/14/2020	P. Luce		Edits
0.92	9/29	C. Lidz		Edits and Comments
0.93	10/10	C. Nersisyan		Adjustments based on C. Lidz comments
0.94	10/21/20	C. Nersisyan		Removed IT responsibility of setting up initial users

Purpose:

This document describes protocols to be followed by the Los Angeles Community College (LACCD) when creating and using MS Teams and SharePoint 365 sites. MS Teams and SharePoint are collaboration tools provided by Microsoft with the District's Office 365 Subscription. The two tools are used in different ways and for different purposes.

Microsoft Teams

MS Teams has no granular security or restrictions, allowing for full and open sharing within the MS Teams group. It is more appropriate for having group chats, meetings, and group file sharing for collaboration with the entire team.

Microsoft SharePoint

SharePoint allows for more granular access permissions and provides greater control over security. SharePoint is more appropriate where file uploads, storage and individual restrictions are required.

Scope:

The scope of this document is in reference to MS Teams and SharePoint online within LACCD's Office 365 tenancy. It covers three levels of collaboration tools, all of which will be restricted to internal users within the organization, with limited exceptions made on a case by case basis. The 3 levels of collaboration tools are:

- MS Teams (no PII* permitted)
- SharePoint Site (no PII* permitted)
- Secure SharePoint Site (PII* permitted by CIO approval)

*PII is "Personally Identifiable Information" that can personally identify an individual, and is protected by laws that include, but are not limited to the Family Education Rights and Privacy Act (FERPA), the Graham Leech Bliley Act (GLBA), and the California Information Practices Act (California Civil Code § 1798 et. seq.). Examples include student/employee social security numbers, dates of birth, driver's license numbers, educational records, health records, and financial aid information.

Roles:

Business Roles:

Role	Key Responsibilities
Department Head Sponsor	Serves as the centralized, primary role for ensuring that content for a particular site is properly collected, reviewed, published, and maintained over time. The Department Head Sponsor will determine the need for sites within their department and will be the single point of contact for requesting the creation and deletion of sites from IT. They will define the Team Owner, initial users, and type of site required. The department head is also responsible for assuring MS Teams and/or SharePoint sites do not contain unapproved PII.
Team/Site Owner	Serves as the primary role for ensuring that content for a particular site is properly collected, reviewed, published, and maintained over time. The Team Site Owner is an expert in the content that is showcased on the site. Manages the site day-to-day by executing the functions required to ensure that the content on the site is accurate and relevant. Manage group membership of the site as appropriate (for sites with no PII). Monitors site security to ensure that the security model for the site matches the goals of the business need and supports users of the site by serving as the primary identified contact point for the site. Acts as the Content Steward for the sites for which they are responsible. Ensures approved PII is stored appropriately.
Users	Uses the solution to access and share information. Users may have different access permissions in different areas of the solution, sometimes acting as a Contributor (content producer) and other times acting as a Visitor (content consumer).

Technical Roles:

Role	Key Responsibilities
Global Admin	Serves as the centralized, primary role for maintaining Office 365 infrastructure. Overall responsibility for ensuring proper usage and creation of sites by technical team. Global admins will be the only group able to create SharePoint sites that will contain PII and will manage group membership for sites that contain PII. Global admins will also be able to add guests to sites on a minimal case-by-case basis. This function will be served by the ESC SSE team.
SharePoint Admin	Serves as the primary role for local requests of site creations. Will be responsible for technical creation of the site and initial setup of Site owner. This function will be served by the Web Architecture team.
MS Teams Admin	Serves as the primary role for local requests of MS Teams creations. Will be responsible for technical creation of the team and initial setup of team owner. This function will be served by the local college or ESC Exchange admin
Local IT Support Team	Provides end user support to users, Team Site Owner, and Department Head Sponsors. Assistance includes, login assistance, assigning permissions for elevated business users, and general guidance. Support does not include maintaining the site or designing it. This team will be served by IT agents who will be identified by Local and Regional College IT Managers

Protocol 1: MS Teams Site (no PII permitted)

Site Usage and Limitations:

Microsoft Teams is a chat-based workspace application that's meant to be used for collaborating and communicating within your organization. It is intended to be as seamless as possible with other Office365 tools with minimal overhead. No PII is allowable in MS Teams.

Microsoft Teams has security limitations that make it ill-suited for highly sensitive documents. All employees should be advised that sensitive documents are not to be stored in Teams for any reason. This includes documents that are confidential for contractual reasons, and documents that contain PII.

Guest Access (Users outside LACCD) is not allowed on MS Teams. MS Teams should be used where you need to conduct:

- Conversations

- Share Files with everyone with no restrictions.
- Private Chats
- Meetings and Calls

General Conditions:

All MS Team sites are for internal organizational use only. Teams is not intended for student usage or as a classroom tool. MS Teams will be limited to departments and groups. Single users will not be granted an MS Team site. Minimal exceptions may be made to include outside guests and must be approved by the Department Head Sponsor. Guests will be added by Global Admins who are members of the ESC Technical staff.

Site Request and Approval

A MS team may be requested by a sponsoring Department Head using a form authorized by the Office of Information Technology (OIT). The form may be submitted to the OIT help desk for fulfillment without further approvals.

Site Requests and Approval for Student Government Associations

A MS team for a Student Government Associations may be requested by a sponsoring employee representative from the EPIE department. The same form authorized by the Office of Information Technology (OIT) may be used. The form may be submitted to the OIT help desk for fulfillment without further approvals.

User Security Restrictions:

Users being granted access to use MS Teams will be required to register using Azure Multi Factor Authentication (MFA). District email can still be utilized without MFA, however additional security is required due to the nature of SharePoint and MS Teams. MFA via a text, call, or Microsoft Authenticator App will be required whenever accessing SharePoint or MS Teams.

Naming Convention:

Due to the size of the District's MS Teams environment, Team names must adhere to strict naming guidelines to simplify the organization of MS Teams and its administration. Team names will consist of a combination of Site Location, Department, and Purpose:

- Location: Site Acronym (ELAC, LACC, LATTC, LAVC, LAPC, LAMC, LAHC, LASC, WLAC, ESC, VDK, BUILDLACCD)
- Department: Department/Division name (i.e. Accounting, A&R, CFA, IT, Facilities, etc.)
- Purpose: One word defining the purpose of the site or group within the department (i.e. Management, BluePrints, Admins, SystemsEngineers, WebDevelopers, etc.)

The naming format will be as follows: <Location>.<Department>.<Purpose>. If a site is meant to be shared across multiple locations, "LACCD" will be utilized as the location name.

Member Management:

Department Head Sponsors will designate a Team Owner who is also a member of the team. The site's Team Owner will be able to add or remove members from the team as required.

Site Markings/Watermarks

No special site markings or watermarks are required for MS Teams sites.

User Training

No special training is required to be a member or Team Owner of a team. Upon creation of a Team, the Team Owner will be provided with a link to general training videos for Microsoft Teams, currently available at: https://support.microsoft.com/en-us/office/microsoft-teams-video-training-4f108e54-240b-4351-8084-b1089f0d21d7.

Security Auditing

The OIT Information Security Office may audit all MS Teams sites, and request PII be removed by the Team Owner. OIT Information Security team may remove documents containing PII and/or disable the MS Team without warning until PII is removed.

Retiring a Site

The sponsoring Department Head may disable or remove a MS Team site by contacting the OIT Help Desk. The OIT may also monitor site utilization and coordinate with sponsoring Department Heads as prudent to verify the activity of MS Teams and remove Teams that are no longer active.

Protocol 2: SharePoint Site (no PII permitted)

Site Usage and Limitations:

SharePoint is a web-based collaborative platform that integrates with Microsoft Office. It allows for storage, retrieval, searching, archiving, tracking, management, and reporting on electronic documents and records. SharePoint contains team collaboration groupware capabilities, including:

- project scheduling
- social collaboration
- shared mailboxes
- project related document storage and collaboration.

Standard SharePoint Sites will not be allowed to contain any confidential information, personal information, or any PII of any sort.

General Conditions:

SharePoint can be used as a collaboration tool to share large files as well as create numerous collaboration tools. Use it as a document repository to store, organize, share, and access files and information that are not managed in another system of record.

Most SharePoint sites will not be allowed to store PII. If a SharePoint site is needed to store PII then a higher level of security will be needed- see Protocol 3.

All SharePoint sites are for internal organizational use only. This is not intended for student usage or as a classroom tool. SharePoint will be limited to LACCD College departments and divisions. Single users will not be granted a SharePoint site.

Site Request and Approval

A standard SharePoint site (no PII permitted) may be requested by a sponsoring Department Head using a form authorized by the Office of Information Technology (OIT). The form may be submitted the OIT help desk for fulfillment without further approvals.

User Security Restrictions:

Users being granted access to use SharePoint will be required to register using Azure Multi Factor Authentication (MFA). District email can still be utilized without MFA, however additional security is required due to the nature of SharePoint and MS Teams. MFA via a text, call, or Microsoft Authenticator App will be required whenever accessing SharePoint or MS Teams.

Naming Convention:

Due to the size of the District's SharePoint environment, site names must adhere to strict naming guidelines to simplify the organization of SharePoint Sites and their administration. Site names will consist of a combination of Site Location, Department, and Purpose:

- Location: SiteAcronym (ELAC, LACC, LATTC, LAVC, LAPC, LAMC, LAHC, LASC, WLAC, ESC, VDK, BUILDLACCD)
- Department: Department/Division name (i.e. Accounting, A&R, CFA, IT, Facilities, etc.)
- Purpose: One word defining the purpose of the site or group within the department (i.e. Management, BluePrints, Admins, SystemsEngineers, WebDevelopers, etc.)

The naming format will be as follows: <Location>.<Department>.<Purpose>

If a site is meant to be shared across multiple locations, "LACCD" will be utilized as the location name.

Member Management:

Department Head Sponsors will designate a Site Owner who is also a member of the team. The Site Owner will be able to add or remove members from the team as required.

Guest Access:

Minimal exceptions may be made to include outside guests and must be approved by the Department Head Sponsor. Guests will be added by Global Admins who are on the ESC Technical staff. Requests for Guest access can be made by using the Guest Request Form.

Site Markings/Watermarks

No special site markings or watermarks are required for SharePoint sites that do not contain PII.

User Training

No special training is required to be a member or Site Owner of a standard SharePoint site. Upon creation of a SharePoint Site, the Site Owner will be provided with a link to general training videos for Microsoft SharePoint Online, currently available at: https://support.microsoft.com/en-us/office/sharepoint-video-training-cb8ef501-84db-4427-ac77-ec2009fb8e23 .

Security Auditing

The OIT Information Security Office may audit all MS SharePoint sites, and request PII be removed by the Site Owner. OIT Information Security team may remove documents containing PII and/or disable the MS Team without warning until PII is removed.

Retiring a Site

The sponsoring Department Head may disable or remove a SharePoint site by contacting the OIT Help Desk. The OIT may also monitor site utilization and coordinate with sponsoring Department Heads as prudent to verify the activity of sites and remove sites that are no longer active.

Protocol 3: Secure SharePoint Site (PII permitted by CIO approval)

Site Usage and Limitations:

SharePoint is a web-based collaborative platform that integrates with Microsoft Office. It allows for storage, retrieval, searching, archiving, tracking, management, and reporting on electronic documents and records. SharePoint contains team collaboration groupware capabilities, including:

- project scheduling
- social collaboration
- shared mailboxes
- project related document storage and collaboration.

General Conditions:

SharePoint sites containing PII must be limited in number of sites and number of users with access. Duplicate sources for the same PII must be minimized or eliminated. Guest access will *NOT* be allowed to SharePoint sites containing any PII. This is not intended for student usage or as a classroom tool. SharePoint will be limited to departments and groups. Single users will not be granted a SharePoint site.

Site Request and Approval

A SharePoint site which will contain PII may be requested by a sponsoring Department Head using a form authorized by the Office of Information Technology (OIT). The form may be submitted the OIT help desk for fulfillment. Additional approval will be required by the Vice Chancellor/CIO.

User Security Restrictions:

Users being granted access to use SharePoint will be required to register using Azure Multi Factor Authentication (MFA). MFA via a text, call, or Microsoft Authenticator App will be required whenever accessing SharePoint or MS Teams.

Where feasible, the OIT shall restrict MFA logins to SharePoint sites with PII in a manner that assures users connect from within the United States of America. If a user is located outside the United States of America, limited exceptions may be granted for a finite amount of time and shall be evaluated on a case-by-case basis.

Naming Convention:

Due to the size of the District's SharePoint environment, site names must adhere to strict naming guidelines to simplify the organization of SharePoint Sites and their administration. Site names will consist of a combination of Site Location, Department, and Purpose:

- Location: SiteAcronym (ELAC, LACC, LATTC, LAVC, LAPC, LAMC, LAHC, LASC, WLAC, ESC, VDK, BUILDLACCD)
- Department: Department/Division name (i.e. Accounting, A&R, CFA, IT, Facilities, etc.)
- Purpose: One word defining the purpose of the site or group within the department (i.e. Management, BluePrints, Admins, SystemsEngineers, WebDevelopers, etc.)

The naming format will be as follows: <Location>.<Department>.<Purpose>.Confidential
If a site is meant to be shared across multiple locations "LACCD" will be utilized as the location name.

Member Management:

Department Head Sponsors will designate a Site Owner who is also a member of the site. The Site's Owner will be able to add or remove members from the team as required. The site owner is responsible for maintaining the membership and limiting access to the confidential site (with sensitive or PII data) only to the staff that absolutely require access to perform their duties. The members should be immediately removed as soon as the collaboration project is completed or the person no longer serves in a capacity which requires them access to the information.

Site Markings/Watermarks

Special site template(s) and/or watermarks are required for SharePoint Sites containing PII. The watermarks or templates will be applied by OIT and may not be removed.

Encryption

All documents containing PII stored on a SharePoint site shall be encrypted at all times. The OIT Information Security Office may encrypt documents containing PII that were not encrypted by the user at any time without warning.

PII Limitations

Any single document containing approved PII shall contain PII for no more than 499 individuals. The OIT Information Security Office may remove or lock any document found containing PII for more than 499 individuals without warning to the users.

User Training

Special training is required to be a member or Site Owner of a SharePoint site containing PII. In addition to standard training recommended for SharePoint, all members must be trained by the ESC IT and Security teams.

Security Auditing

The OIT Information Security Office will audit all SharePoint sites containing PII. The OIT Information Security team may freeze or remove sites if evidence of misuse is found or no recent activity.

Retiring a Site

The sponsoring Department Head may remove a SharePoint Site containing PII by contacting the OIT Help Desk. The OIT may also monitor site utilization and coordinate with sponsoring Department Heads as prudent to verify the activity of SharePoint sites and remove those that are no longer active. OIT Information Security team

Procedures:
(To be developed after protocols are approved).

Related Documents:

Collaboration Site Request Form for SharePoint and MSTeams:

LACCD.CollaborationSiteRequestForm_v1_2020_10_20.xlsx

Guest Access Request Form:

LACCD.MsoftGuestRequestForm_v1_2020_10_20.xlsx