BY ORDER OF THE COMMMANDER
JOINT BASE ELMENDORF-RICHARDSON

JOINT BASE ELMENDORF RICHARDSON INSTRUCTION 33-300

5 JANUARY 2024

Communications and Information

ENTERPRISE INFORMATION MANAGEMENT—SHAREPOINT®

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-Publishing.af.mil** for downloading and ordering

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: 673CS/SCXK

Certified by: 673CS/CC
(Lt Col Christopher L. Foltz)

Supersedes: JBElmendorf-RichardsonI33-300, 12 August 2019

Pages: 9

This instruction implements Air Force Policy Directive (AFPD) 33-3, *Information Management*. It outlines guidance and procedures on Joint Base Elmendorf-Richardson's (JBER) Enterprise Information Management (EIM) SharePoint® processes. This instruction applies to all Air Force personnel, supported tenant organizations, and mission partners who utilize the installation's SharePoint® site collection to include the Air Force Reserve and Air National Guard. This publication may not be supplemented at any level. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) listed above using the Department of the Air Force (DAF) Form 847, *Recommendation for Change of Publication*; route DAF Forms 847 from the field through the appropriate chain of command. Submit requests for waivers through the chain of command to the publication OPR for non-tiered compliance items. Ensure that all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction (AFI) 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the DAF.

SUMMARY OF CHANGES

This publication has been substantially revised and needs to be completely reviewed. Major changes include expanded roles and responsibilities, site collection information, and updated definitions.

1. Overview.

1.1. SharePoint® is a standardized electronic collaborative environment for personnel to share and acquire information and knowledge. The mission of EIM is to provide the right information to the right individuals to support combat and mission operations through a single common platform and standardized business processes. SharePoint® is JBER's primary tool for management of document libraries, workspaces, and workflows. This instruction outlines the objectives, roles, responsibilities, permissions, requirements, policies, and security necessary to support sites within JBER's site collection, managed by the 673d Communications Squadron Knowledge Management Center (CS/SCXK).

1.2. JBER Customer Base. The customer base for SharePoint® includes both Wings, units, and tenants supported by the Non-Secure Internet Protocol Router (NIPR) and Secure Internet Protocol Router (SIPR) Networks.

1.3. Classification. The NIPR SharePoint® and Intelink environment is authorized to store data up to "Controlled Unclassified Information (CUI)". The SIPR SharePoint® and Intelink environment is authorized to store data up to "Secret".

1.3.1. All site content within JBER's site collection will be clearly marked and protected in accordance with Department of Defense Manual (DoDM) 5200.01 Volume 1_Air Force Manual (AFMAN) 16-1404 Volume 1, *Information Security Program: Overview, Classification, and Declassification,* and AFI 33-332, *Air Force Privacy and Civil Liberties Program.*

1.3.2. Appropriate marking of documents, items, and security of controlled unclassified information and classified material maintained on sites, lists, and document libraries are the responsibility of the information owner.

1.4. Intelink operates in a SharePoint® environment. All JBER Intelink sites will comply with the same guidance and acceptable use policies that are laid out in this publication and be referred to as SharePoint® site, unless stated otherwise.

2. Roles and Responsibilities.

2.1. Commanders and Heads of Wing Staff Agencies:

2.1.1. Appoint in writing a primary and alternate Content Manager to manage their site. Send appointment letter to the Knowledge Management Center (KMC) organizational email box at: **673cs.eis@us.af.mil**.

2.1.1.1. Content Managers will be replaced at least 30 days prior to departure due to permanent change of station (PCS), permanent change of assignment (PCA), retirement, or separation to allow sufficient time for training and integration into the program.

2.2. 673d Communications Squadron Commander (CS/CC) appoints in writing primary and alternate(s) Site Collection Administrators (SCA).

2.3. The 673 CS/SCXK:

2.3.1. Oversees the JBER EIM—SharePoint® environment.

2.3.2. Serves as the base SCAs for all sites under JBER's site collection. SCAs manage the layout, structure, design, permissions, and operations. (**Note:** SCAs will not grant permissions to End Users, as this is the Content Manager's and Subsite Content Manager's responsibility.) SCAs will:

2.3.2.1. Manage JBER's site collection on SharePoint® and Intelink.

2.3.2.2. Establish local training sessions using official guidance and requirements.

2.3.2.3. Provide training for Content Managers and Subsite Content Managers.

2.3.2.4. Grant "Full Control" permissions to appointed and trained Content Managers.

2.3.2.5. Upon request, assist Content Managers on creating sites, assigning permissions, resolving issues, and developing standardized solutions.

2.3.2.6. Remove "Full Control" permissions from top-level site collections for any unit or Staff Agency that granted "Full Control" to an individual not identified on the Unit Content Manager or Subsite Content Manager appointment letter.

2.4. Flight Directors/Commanders/Chiefs, Work Center Supervisors, Private Organization President or Vice President, and Ranking Person of Special Program or Project will:

2.4.1. Request site creation from unit Content Manager as needed.

2.4.2. Appoint or assign Subsite Content Managers.

2.5. Content Managers and Subsite Content Managers:

2.5.1. Manage their unit's SharePoint® site and all content that falls under their site and have "Full Control" permissions for their site, subsites, lists, libraries, pages, and other content that falls under their purview.

2.5.2. Complete SharePoint® Content Manager training provided by 673 CS/SCXK within 30 days of appointment.

2.5.3. Manage subsites and content.

2.5.4. Ensure stagnant information is removed from site, to include broken links.

2.5.5. Grant permissions to end users via SharePoint® Groups or Active Directory Security Groups to assign permissions on all sites and site assets as appropriate based on permission level needed to meet mission requirements. Individual permissions are not assigned, instead permissions are granted to SharePoint groups and individuals are added to the groups.

2.5.6. Ensure SharePoint® Groups are maintained and ensure personnel are removed or added as they PCS or PCA.

2.5.7. Perform monthly scans of SharePoint® and/or Intelink sites.

2.5.8. Content Managers:

2.5.8.1. Maintain subsites under their organization's site collection.

2.5.8.2. Grant "Full Control" permissions to appointed Subsite Content Managers after they have attended training with 673 CS/SCXK.

2.5.8.3. Assist Subsite Content Managers on creating sites, assigning permissions, resolving issues, and developing standardized solutions upon request.

2.5.8.4. Maintain a list of Subsite Content Managers within their organization.

2.5.8.5. Contact the 673 CS/SCXK SCAs for assistance as needed.

2.5.8.6. Remove "Full Control" permissions from any subsite for an individual or group that contains individuals not identified as Subsite Content Managers on that subsite.

2.5.9. Subsite Content Managers:

2.5.9.1. Request site creation from organization's Content Manager.

2.5.9.2. Ensure unit Content Manager's SharePoint® group has "Full Control" to subsite and all subsite assets.

2.5.9.3. Contact their unit Content Manager for assistance as needed.

2.6. End Users:

2.6.1. End users must understand their role in maintaining current information on SharePoint® as well as ensuring the security of information on SharePoint® regardless of their granted permission level or ability to add, edit, delete, or just read information.

2.6.2. Must immediately report any unauthorized access to Privacy Act/Personally Identifiable Information (PA/PII) material to their Unit's Privacy Monitor, whom will in turn report the violation to the Base Privacy Manager.

2.6.3. Contact unit Content Manager or Subsite Content Manager prior to posting CUI to SharePoint® to ensure that it is posted to an area restricted to only those who have a valid need to know to conduct official business.

2.6.4. Do not load publications, Technical Orders (TOs), or other documents where the originals are maintained on other government sites. Instead utilize links to the documents so current information is always accessible.

2.6.5. Do not use unit's SharePoint® site as a personal repository. Unit SharePoint® sites are for unit mission needs.

2.6.6. Request access to SharePoint® sites and content from Content Managers or Subsite Content Managers.

3. Sites. SharePoint® places the management of content firmly in the hands of site owners and their end users. The portal concept of users as content managers is a privilege that gives organizations flexibility to create and maintain information as they see fit.

3.1. All sites must have the Content Manager's contact information visible on the main page.

3.2. Sites not visited for at least 180 days are subject to deletion. Content Managers will be notified via e-mail 10 duty days prior to deletion.

3.3. Site Types:

3.3.1. Organization Sites. Typically wing, unit, flight, element, and work center sites. Referred to as the unit's site. All unit's respective sites are on the JBER site collection. The JBER site is the top-level site for the 673d Air Base Wing (ABW), 3d Wing (WG), and tenant units and is the only site collection. Individual units do not have separate site collections.

3.3.2. Subsites. Organization Subsites can be built for each letter organization as needed and required; however, the sites should be maintained at the highest level possible to prevent duplication of content. Subsites should be nestled under the organization's top-level site to maintain a consistent structure.

3.3.3. Community Sites. Developed to accommodate project collaboration for multiple users across multiple organizations. Community sites allow for permissions to be granted to users in different organizations without modifying the permissions of parent sites.

3.3.3.1. Community sites should not be nested under an organization's site. Users wanting a community site created should request through 673 CS/SCXK by emailing the organizational email box at: **673cs.eis@us.af.mil**.

3.3.3.2. The executive council for base private organizations will assume site ownership upon election. Elected council is required to contact 673 CS/SCXK to schedule training before receiving full control of their site.

4. Permissions. Management of security for a SharePoint® site is the responsibility of the content managers at all levels. Permissions will be assigned directly to active directory groups or through a SharePoint® group.

4.1. Default security groups for JBER's site collection are owners, members, and visitors. Use default groups to maintain consistency across the collection as this ensures permissions are up to date as personnel changes occur.

4.1.1. Content Managers will have "Full Control" of the site they're appointed to. Full Control allows content managers to create, maintain, and delete site content and subsites within their collection. Additionally, Content Managers can grant permissions to End Users who require access to their content.

4.1.2. Site members will have Contribute rights. This allows assigned individuals to view, add, update, and delete list items and documents. **Note**: when creating new member groups, ensure the contribute level is selected as the edit level tends to be the default.

4.1.3. Site visitors will only be able to view pages and list items and download documents.

4.2. All material maintained on SIPR will contain the appropriate classifications, caveats, and be labeled accordingly with the proper access controls and/or restricted permissions in place.

5. Prioritization of Work Requests.

5.1. The following command levels will be considered when prioritizing work requests:

5.1.1. Wing CC and Staff.

5.1.2. Group CC and Staff.

5.1.3. Squadron CC.

5.2. Projects that have a significant impact on the base populace or critical missions will take precedence. This will be determined by the 673 CS/SCXK, with guidance from flight and squadron leadership.

5.3. Completion timelines. Standard site creation will take up to 10 duty days. Sites requiring additional features or coding/scripting may take longer. 673 CS/SCXK will communicate this to the customer after reviewing the request and gathering any additional requirements.

DAVID J. WILSON, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoDM 5200.01V1_AFMAN 16-1404V1, *Information Security Program: Overview, Classification, and Declassification,* 6 Apr 2022

AFPD 33-3, *Information Management*, 8 Sep 2011

AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020

AFI 33-332, *Air Force Privacy and Civil Liberties Program*, 10 Mar 2020

Prescribed Forms

None

Adopted Forms

DAF 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

CUI—Controlled Unclassified Information

DAF—Department of the Air Force

DoDM—Department of Defense Manual

EIM—Enterprise Information Management

JBER—Joint Base Elmendorf-Richardson

NIPR—Non-Secure Internet Protocol Router

OPR—Office of Primary Responsibility

PA—Privacy Act

PCA—Permanent Change of Assignment

PCS—Permanent Change of Station

PII—Personally Identifiable Information

SCA—Site Collection Administrator

SIPR—Secure Internet Protocol Router

TO—Technical Order

Office Symbols

ABW—Air Base Wing

CS/CC—Communications Squadron Commander

CS/SCXK—Communications Squadron Knowledge Management Center

WG—Wing

Terms

Content Manager—A group or individual who can create lists and libraries, contribute to lists and libraries, and assign user permissions.

Controlled Unclassified Information (CUI)—Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and government-wide policies.

End User—Anyone with the ability to access JBER's site collection.

Site Collection—A top-level site that can store a group of sub-sites, document libraries, calendars, and lists that is maintained by the appointed/assigned content managers.

Site Owner—Group or individual who has full control of a top-level site and all its subsites.