BY ORDER OF THE COMMANDER
MACDILL AIR FORCE BASE (AMC)

MACDILL AIR FORCE BASE
INSTRUCTION

33-301

13 MAY 2019

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 or ordering

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: 6 CS/SCXK

Certified by: 6 CS/CC
(Lt Col Estelle)

Pages: 15

This publication implements Air Force Policy Directive (AFPD) 33-3, *Information Management*. It provides guidance and procedures on MacDill Air Force Base's (AFB) Enterprise Information Management (EIM) SharePoint® process. It applies to the 6th Air Mobility Wing (6 AMW), and mission partners, military, civilian, and contractor personnel who utilize MacDill AFB's EIM-SharePoint® environment. This publication may be implemented or supplemented at any level, but all such publications and/or supplements must be routed to the Office of Primary Responsibility (OPR) listed above for coordination prior to certification and approval. Refer recommended changes and questions about this publication to the OPR listed above using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See AFI 33-360, Publications and Forms Management, **Table 1.1** for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items. 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 Air Force.

1. Overview. This Instruction provides guidance and procedures for the management of MacDill's EIM SharePoint® environment. SharePoint® is a standardized electronic collaborative workplace for Airmen 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 MacDill's primary tool for management of document libraries, document workspaces, and workflows. The SharePoint® environment is not to be used for storage of official files that are required to be maintained on the official records storage drive (O: drive).

2. Roles and Responsibilities.

2.1. The 6th Communications Squadron Commander appoints primary and alternate(s) Base Site Collection Administrators (MacDill SharePoint® Administrators).

2.2. Base Site Collection Administrators/MacDill SharePoint® Administrators (6 CS/SCXK).

2.2.1. Manage MacDill's site collections.

2.2.2. Establish local training sessions using local operating procedures or requirements.

2.2.3. Provide training for Unit Site Owners.

2.2.4. Grant "Full Control" permission to appointed and trained Unit Site Owners.

2.2.5. Upon request, assist Unit Site Owners on creating sites, assigning permissions, resolving issues, and developing standardized solutions.

2.2.6. Provide support to Unit Site Owners for maintaining and administering SharePoint® features, including daily monitoring, troubleshooting, and performance analysis of the system specifically supporting MacDill's capabilities.

2.2.7. Will not grant permissions to End Users, as this is the Unit Site Owner's and Unit Subsite Owner's responsibility.

2.2.8. Will 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 Unit Site Owner appointment letter.

2.3. Commanders and Heads of Wing Staff Agencies.

2.3.1. Appoint in writing a primary and alternate Unit Site Owner to manage their site. Appointment Letters may be created via a Microsoft® Word® document or Adobe® and digitally signed. See **Attachment 3** for Unit Site Owner appointment letter template. Send appointment letter to "6 CS/SCXK SharePoint Admin" organizational email box (**6csscxk.sharepointadmin@us.af.mil**). **NOTE**: Recommend three Unit Site Owners that are on different air expeditionary force (AEF) bands to ensure a site owner is available to manage their site at all times.

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

2.3.1.2. Additional or replacement Unit Site Owners will be appointed if a unit has no Site Owners available for extended periods, due to leaves, temporary duty (TDY), illness, etc., and 6 CS/SCXK must immediately be notified so the new Unit Site Owners can receive training.

2.3.2. Validate/update appointment memos at least annually and as necessary to ensure Unit Site Owners are assigned and there is proper control over the SharePoint® site.

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

2.4.1. Request site creation from Unit Site Owner as needed.

2.4.2. Appoint or Assign Subsite Owners by providing name and the rank, full name, and duty phone to Unit Site Owner.

2.4.3. Maintain site owner appointments to ensure Subsite Owners are assigned and there is proper control over the site.

2.5. Unit Site Owners and Subsite Owners.

2.5.1. Are trusted agents for their 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 site. Their SharePoint® Unit Site Owner Group has "Full Control" to all content throughout their unit's site collection to include team sites that fall under the unit's site collection.

2.5.2. Complete SharePoint® Site Owner training provided by 6 CS/SCXK within 30 days of appointment.

2.5.3. Administer their assigned SharePoint® site's day-to-day administration and support.

2.5.4. Manage subsites and content.

2.5.5. Provide training for end users.

2.5.6. Ensure stagnate information is removed from site.

2.5.7. Grant permissions to users via SharePoint® groups to their site and subsites and to content as appropriate based on permission level needed to meet mission requirements.

2.5.8. Restrict access to For Official Use Only (FOUO) information to only users that have a valid need to know to conduct official business. Refer to **Paragraph 4** for more information about FOUO and the Air Mobility Command (AMC) Enterprise Information Management (EIM), Privacy Act Manual for Site Owners located at **https://eim2.amc.af.mil/sites/support/Policy/EIM%20Privacy%20Act.doc** for assistance on setting permissions and breaking permission inheritance.

2.5.9. Use SharePoint® Groups or Active Directory Security Groups to assign permissions on all sites and site assets and ensure SharePoint® Groups are named according to **Attachment 2**. Individual permissions are not assigned, instead permissions are granted to SharePoint groups and individuals are added to the groups.

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

2.5.11. Ensure Official Records are not posted to SharePoint®. SharePoint® is for reference, working drafts, and information not Official Records of the organizations. Official Records must be filed on the O: Drive.

2.5.12. Unit Site Owners.

2.5.12.1. Grant "Full Control" permission to appointed Subsite Owners via Subsite Owner SharePoint® group once Subsite Owner has completed training.

2.5.12.2. Maintain a listing of Subsite Owners by creating lists containing the subsite web address, rank, full name, and duty phone (may be a SharePoint® list) of each Subsite Owner.

2.5.12.3. Assist Subsite Owners on creating sites, assigning permissions, resolving issues, and developing standardized solutions upon request.

2.5.12.4. Provide support to Subsite Owners for maintaining and administering SharePoint® features, including daily monitoring, troubleshooting, and performance analysis of the system specifically supporting MacDill's capabilities.

2.5.12.5. Contact MacDill SharePoint® Administrators for assistance as needed.

2.5.12.6. Remove "Full Control" permissions from any subsite or asset for an individual or group that contains individuals not identified as Subsite Owners on that subsite or subsite asset.

2.5.13. Subsite Owners.

2.5.13.1. Ensure Unit Site Owner's SharePoint® group or Active Directory (AD) Security group has "Full Control" to subsite and all subsite assets.

2.5.13.2. Contact Unit Site Owner for assistance as needed.

2.5.13.3. Remove "Full Control" permissions from any subsite or asset for an individual or group that contains individuals not identified as Subsite Owners.

2.6. End Users.

2.6.1. Are anyone with the ability to access MacDill's SharePoint® environment. 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 on MacDill's SharePoint® sites.

2.6.2. Must immediately report any unauthorized access to Privacy Act/Personally Identifiable Information (PA/PII) material to either their Unit's Privacy Monitor, the Unit's Privacy Monitor for the SharePoint® site where the PA/PII resides or Base Privacy Act Manager.

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

2.6.4. Manage the material put onto their respective sites and ensure the information is accurate and current.

2.6.5. Ensure only working drafts for collaboration and routing or informational copies are posted to SharePoint and that unit or office electronic official records are not maintained on SharePoint® as SharePoint® is not authorized for electronic official records. Remove working drafts once finalized and filed to official records. Electronic official records must be maintained on the O: Drive or an approved official electronic record system.

2.6.6. 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 are used so current information is always accessed.

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

2.6.8. Request access to SharePoint® sites and content from site and subsite owners that own the sites.

3. MacDill's SharePoint® Environment. MacDill's SharePoint® Environment is part of Air Mobility Command's SharePoint® environment and is managed by 6 CS/SCXK.

3.1. Sites.

3.1.1. Organization Sites.

3.1.1.1. Communicate and share information about their specific organization or office across the enterprise or share or collaborate on information internally for their specific organization or office. Organizational sites are typically unit, flight, element, and work center sites.

3.1.1.2. Unit organization sites are referred to as the Unit's site. The Unit's site is a site collection and is the top-level site for each unit. All 6 AMW units have their own site collections and the 927th Air Refueling Wing belongs to the 6 AMW's site collection. Unit's on MacDill that log into the AF network that do not have their own site collection may request a SharePoint® Unit Organization site creation by submitting a ticket to AMC EIM Help site at **https://eim2.amc.af.mil/sites/support/pages/menu.aspx**.

3.1.1.3. Are open to all members of the Organization for information dissemination or for content contribution. Organizational sites can provide their desired level of access to authenticated users not within the Organization, as they deem necessary.

3.1.1.4. Can be built for each letter organization. However, sites should be maintained at the highest level possible to prevent duplication of content. Flight, element, and work center organization sites are subsites of the unit organization site, are created by the unit site owners, and should be nested under their Organization site to maintain a consistent architecture.

3.1.2. Team Sites. A Team site is created to accommodate a program or project collaboration for multiple users across multiple Organizations or internally. Team sites allow permissions to be granted to users across multiple organizations without modifying

the permissions of the Organizational site. Programs or projects within Team sites are considered anything that is not directly related to the overall daily business of the Organization. When you build a site using a SharePoint® Workspace template, you are building a Team site.

3.2. Web Parts. Third party web parts are not authorized. Third party web parts can have hidden malicious code, contents, and pose a security threat to our network. If a third party web part is required, site owners must submit request to AMCs EIM Support Site, **https://eim2.amc.af.mil/sites/support/pages/menu.aspx**, for approval.

3.3. Master page editing is not authorized. AMC uses the site templates, which restrict the ability to edit master pages. The elements provided by AMC are generic enough to accommodate both AMC and tenant organizations.

3.4. Themes. Site Owners and Subsite Owners are authorized to change themes, styles, background colors, borders, or other page elements, however, it is discouraged in order to keep all MacDill AFB pages colors uniformed across the organizational site collections.

3.5. SharePoint® Designer. Microsoft SharePoint® Designer is not authorized. Improper use of SharePoint® Designer by Site Owners, Subsite Owners, or End-users can cause system malfunctions.

3.6. Site Content & Management.

3.6.1. To avoid the stagnation of information within the environment, organizations must ensure the accuracy and relevancy of information within their sites.

3.6.2. Site owners and Subsite owners need to monitor their sites activity. Site and subsite owners should validate sites and/or contents are still needed on sites and workspaces inactive for 90 days or longer.

3.6.3. All MacDill SharePoint® sites will exclude content that falls within the following categories:

3.6.3.1. SharePoint® is not authorized for storage of official records. All electronic official records must be stored on the O: Drive or on approved electronic record systems.

3.6.3.2. Technical Orders, Publications, Operating Instructions, or blank Government Forms are not authorized on MacDill's SharePoint® sites. Sites may have links to the official sites for the official published versions of these products. MacDill's Base Publications and Forms Office SharePoint® site (**https://eim2.amc.af.mil/org/6cs/SCX/SCXK/Publications/default.aspx**) is authorized to distribute MacDill's publications and forms via SharePoint®.

3.6.3.3. Do not load documents, slides, pictures, or other files that can be found on other government sites. Instead create a link to the file with a description by having site or Subsite Owners add a "Summary Link Web Part" to the page.

3.6.4. Use the SharePoint® built-in recycle bin to restore an accidentally deleted file. The data will remain in the recycle bin for 30 days.

3.6.5. Files that may cause system vulnerabilities or security risks are blocked and cannot be uploaded to the system. Upload of a blocked file will result in a Warning

Notice. By default, several standard file extensions are blocked, including any file extensions that are treated as executable files by Windows Explorer.

3.6.6. The default maximum upload size of a file is 50MB. To request to load files larger than 50MB submit via AMC's help site, **https://eim2.amc.af.mil/sites/support/pages/menu.aspx**.

3.6.7. All sites will have site owner or Subsite Owner contact information displayed.

4. For Official Use Only Information (FOUO).

4.1. FOUO is a dissemination control applied by the Department of Defense to unclassified information when disclosure to the public of that particular record, or portion thereof, would reasonably be expected to cause a foreseeable harm to an interest protected by one or more of Freedom of Information Act (FOIA) Exemptions 2 through 9. **NOTE**: SharePoint® is not publicly accessible, however, if you have information that is covered by one or more of the FOIA exemptions, it is still FOUO information and it must be secured. The FOIA nine exemptions are:

4.1.1. Exemption 1. Classified information and classified information is not allowed on MacDill's SharePoint Environment.

4.1.2. Exemption 2. Information that pertains solely to the internal rules and practices of the agency that, if released, would allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission. Exemption 2 is rarely applied anymore, consult legal if in doubt as to whether or not this exemption applies.

4.1.3. Exemption 3. Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed. A listing of the statues is at **http://www.foia.af.mil/Portals/22/documents/AFD-141010-017.pdf**.

4.1.4. Exemption 4. Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the Government's ability to obtain like information in the future, or impair the Government's interest in compliance with program effectiveness.

4.1.5. Exemption 5. Inter- or intra-agency memorandums or letters containing information considered privileged in civil litigation. The most common privilege is the deliberative process privilege, which concerns documents that are part of the decision-making process and contain subjective evaluations, opinions, and recommendations. Other common privileges are the attorney-client and attorney work product privileges.

4.1.6. Exemption 6. Information, the release of which would reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals. This is more commonly referred to as Personally Identifiable Information (PII) or information covered by the Privacy Act (PA).

4.1.6.1. PII is defined as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful

permanent resident, visitor to the U.S. or employee or contractor to the Department of Defense.

4.1.6.2. PII data and documents that contain personal information protected under the PA. Information such as recall rosters, personnel rosters, lists or spreadsheets shall be marked "FOR OFFICIAL USE ONLY" and shall contain the following statement: "The information herein is For Official Use Only (FOUO) which must be protected under the Freedom of Information Act of 1966 and Privacy Act of 1974, as amended. See AFI 33-332, *Air Force Privacy and Civil Liberties Program* and DoDM 5200.01, Volume 4, *DoD Information Security Program*, for proper marking and handling of FOUO material. Once the PII data is no longer needed the individual, who posted the information must ensure the PII data is removed. Common examples of PII are listed below:

4.1.6.2.1. Social security number (SSN) to include just the last 4.

4.1.6.2.2. Driver's license or state identification number.

4.1.6.2.3. Passport number.

4.1.6.2.4. Biometric identifiers (e.g., fingerprint, iris scan, voiceprint).

4.1.6.2.5. Credit card account number.

4.1.6.2.6. Home address.

4.1.6.2.7. Home or cell phone.

4.1.6.2.8. Full date of birth.

4.1.6.3. Site owners and site managers must have a heightened awareness of high-impact PII stored and accessed through SharePoint®. Access to documents containing PII should never be given to groups of individuals unless each person has an official need to know the information to conduct official business. See AFI 33-332, **Paragraphs 2.2.1.8** and **2.2.1.10**.

4.1.7. Exemption 7. Records or information compiled for law enforcement purposes that:

4.1.7.1. Could reasonably be expected to interfere with law enforcement proceedings.

4.1.7.2. Would deprive a person of a right to a fair trial or impartial adjudication.

4.1.7.3. Could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others.

4.1.7.4. Disclose the identity of a confidential source.

4.1.7.5. Disclose investigative techniques and procedures.

4.1.7.6. Could reasonably be expected to endanger the life or physical safety of any individual.

4.1.8. Exemption 8. Certain records of agencies responsible for supervision of financial institutions.

4.1.9. Exemption 9. Geological and geophysical information (including maps) concerning wells.

4.2. FOUO information should not be stored on SharePoint unless it is required for daily business or mission requirement and is only accessible to the individuals who need the information to perform AF business.

4.3. Individuals who post FOUO information to SharePoint® must include "(FOUO)" preceding the subject title and/or the folder title (e.g., (FOUO) Recall Roster, (FOUO) AF910 Draft EPR - A1C Smith, etc.). See DoDM 5200.01, Volume 4, for proper marking of FOUO material.

4.4. Remove FOUO information from SharePoint once it has served its purpose to avoid unnecessary risk of possible access or possible PII breach or PA violation.

4.5. End users will contact Site or Subsite Owners prior to loading any FOUO material to SharePoint® to ensure it is loaded to a secure area or it is secured as it is loaded. Site Owners will provide user assistance in locking down FOUO content by creating separate permission groups specifically for FOUO, however, ultimately the user is responsible to ensure FOUO is secured.

5. Records Management. Records play a vital role in managing and operating Air Force activities. MacDill's SharePoint® is not authorized to store official records and is not an official records repository. Manage official records according to AFI 33-322, *Records Management Program*, AFI 33-364, *Records Disposition—Procedures and Responsibilities*, AFMAN 33-363, Air Force *Electronic Records Management (ERM) Solution*, and 6 AMW Records Management Plan. Contact your local Records Inventory Manager and/or supervisor for specific office filing procedures.

STEPHEN P. SNELSON, Colonel, USAF
Commander, 6th Air Mobility Wing

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

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

AFI 33-322, *Records Management Program*, 4 June 2012

AFMAN 33-363, *Management of Records*, 1 March 2008

AFI 33-364, *Records Disposition—Procedures and Responsibilities*, 22 December 2006

AFI 33-332, *Air Force Privacy and Civil Liberties Program*, 12 January 2015

DOD5400.7-R_AFMAN33-302, *Freedom of Information Act Program*, 21 October 2010

DoDM 5200.01, Volume 4, *DoD Information Security Program*, 24 February 2012

Air Mobility Command, *Enterprise Information Management (EIM), Privacy Act Manual for Site Owners*, 16 June 2009

Air Mobility Command, *Enterprise Information Management (EIM), SharePoint 2013 Training Manual for Site Owners and Users*, 21 September 2018

Air Force *Electronic Records Management (ERM) Solution* V7.4, 4 September 2007

Prescribed Forms

None

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

6 AMW—6th Air Mobility Wing

6 CS/SCK—6th Communications Squadron, Knowledge Operations

AD—Active Directory

AEF—Air Expeditionary Force

AFB—Air Force Base

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFRIMS—Air Force Records Information Management System

AMC—Air Mobility Command

EIM—Enterprise Information Management

FOUO—For Official Use Only

MB—Megabyte

OPR—Office of Primary Responsibility

OI—Operating Instruction

PCA—Permanent Change of Assignment

PCS—Permanent Change of Station

PII—Personally Identifiable Information

RDS—Records Disposition Schedule

RSS—Really Simple Syndication

SSN—Social Security Number

TO—Technical Order

Terms

Collaboration—Collaborative tools facilitate the interaction among two or more individuals and encompass a variety of behaviors, including communication, information sharing, coordination, cooperation, problem solving, and negotiation.

Documents—After documents have been added to a document library you can edit the documents, use the Check In/Check Out feature and view all versions of a document. If you cannot perform any of these processes, you may not have permission and should contact your site owner.

Documents Library—Document libraries are the most general form of libraries, being able to store virtually any type of Microsoft Office® document.

Enterprise Information Management—The vision for Enterprise Information Management (EIM) is to provide decision-makers and all AF personnel with on-demand access to authoritative, relevant, and sufficient information to perform their duties efficiently and effectively. The AF EIM tool suite encompasses commercial off the shelf software products that will span all phases of the information management lifecycle, from creation to disposition. It will integrate workflow, document management, content management, electronic records management, and information management tools, and be accessible through and operate on the Global Combat Support System Air Force (GCSS-AF).

For Official Use Only—Information that is covered by one of the nine exemptions of the Freedom of Information Act.

Library—An area where a collection of files is stored. The two types of libraries available are document libraries and picture libraries.

List—A list is a collection of information items displayed in an area or on a site. List types include: announcements, links, contacts, events, tasks, and issues. Custom lists can be created to store many other kinds of information.

Master Page—-Master Pages are a template that other pages can inherit from to keep consistent functionality. The pages that inherit from Master Pages are referred to as content pages. Master Pages allow the developer to keep consistent, reusable, in one high level place, so the content pages can concentrate on their specific web-based code. This allows for easily manageable web-based applications.

Personally Identifiable Information (PII)—Any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S. or employee or contractor to the Department of Defense.

Really Simple Syndication—This is a web format for publishing updated works (e.g., blog entries, news headlines, audio, and video) in a standard format. Really Simple Syndicated (RSS) Feeds are a Web service for providing RSS content. Most all web sites that provide news or online publications provide RSS Feeds.

Recycle Bin—The SharePoint **Recycle Bin** is the storage location where deleted files go. When you delete items on your SharePoint site, go to the **Recycle Bin,** and can be restored for up to 30 days by users. **NOTE**: Documents will be restored back to their original location. Site owners also have the ability to view the recycle bins of other users.

SharePoint®—Is a Microsoft® commercial off-the-shelf product used by MacDill AFB as a standardized electronic collaborative workplace for Airmen to share and acquire information and knowledge.

Site Collection—A top-level site that can store a group of subsites, document libraries, calendars, and lists that is maintained by the site owner(s).

Site Owner—Has full control of a top-level site and all of its sub-sites.

Subsite—A separate site, with individual permissions and content, stored within a site collection (top-level site).

Themes—SharePoint themes represent a collection of graphics and cascading style sheets that can modify how a Web site looks. The SharePoint site settings interface provides the ability for both site administrators and site owners to customize the look and feel of their site by selecting from a pre-defined list of available site themes.

Third Party Software—Software developed by vendors.

Types of Site Content—There are two basic types of content in a SharePoint site: lists and libraries.

Web Part—A customizable web page element that is typically used to display data from lists and libraries on site pages.

Workflow—A workflow is a natural way to organize and run a set of work units, or activities, to form an executable representation of a work process. This process can control almost any aspect of a work unit to include the life cycle. The workflow is flexible enough to model both the system functions and the human actions necessary for the workflow to complete.

Attachment 2

SHAREPOINT GROUP NAMING CONVENTION

Figure A2.1. SharePoint Group Naming Convention

SharePoint® Group Levels	Naming convention	Examples
Wing, Group, and Squadron Site Collections	Wing, Group, or Squadron Number Wing Group, or Squadron Acronym Office Acronym (if applicable) Type of group	6 AMW Owners (Note 1) 6 CS Designers (Note 2) 6 MDG Approvers (Note 3) 310 AS Members (Note 4) 927 MSG Visitors (Note 5) 6 AMW CCE Members 6 OG CSS Members 6 LRS CSS Visitors
Wing Staff Agencies Site Collections	Wing Number Wing Acronym Office Acronym Type of group	6 AMW XP Owners 6 AMW HC Designers 6 AMW DS Approvers 6 AMW PA Members 6 AMW SE Visitors 6 AMW XPI Members 6 AMW First Sergeants Members
Sub Organization Sites – Flight, Element, and Work Center Level	Unit Number Wing, Group, or Squadron Acronym Flight, Element, or Work Center Acronym Type of group	6 CS SCX Owners 6 CS SCO Members 6 CS CCC Visitors 6 CS SCXK Owners 6 CONS LGC Members 6 CS CCC Visitors
Other Team Sites (e.g. Booster Club, Airman Council, Fitness site)	Unit Number Wing Group, or Squadron Acronym Name of group Type of group	6 CS Booster Club Owners 6 MXG Amn Council Members 6 SFS PTL Visitors 6 AMW Top III Visitors 6 CS FOIA Mgrs Members
Asset Group (e.g. list, library, document that requires a unique or restricted permission group)	Unit Number Wing Group, or Squadron Acronym Flight, Element, or Work Center Acronym (If applicable) Name of group Type of group	6 CS SCXK (Recall Roster) Members 6 AMW CAT Staff Members 6 MDG GCC Members 6 MSG UCC Members

NOTES:

Note 1: Owners group names are designated for the site owners and Subsite Owners only and are given "Full Control" to the site. No other groups or personnel will be given "Full Control to a unit's site, subsites, or assets. Each Site Collection and subsite will have only one SharePoint®

Owner Group named for primary management of the site. This does not preclude the responsibilities or removal of the parent SharePoint® Owners group from the site. Do not confuse the "Owners" group with the person who owns the site (e.g. Unit Commander, flight Director/Commander, etc.). Just because they own the site does not authorize them to be in the Owners group; personnel in the Owners group must be appointed and trained.

Note 2: Use "Designers" groups for special teams to customize the look of a site. These groups will be given "Design" rights.

Note 3: Use "Approvers" groups if using SharePoint's® built-in workflows or if workflows are developed that require approval and/or approval is limited to more than just one person.

Note 4: Use "Members" groups for personnel assigned to the Unit (e.g. Wing, Group, Squadron, flight, or office) group. Typically, these groups get "Contribute" permissions to their Unit assets but another work center can give this group "Read" access in the same site collection.

Note 5: Use "Visitor" groups for personnel not assigned to your unit that want to see your site or information on your site. Give "Visitor" groups "Read" permissions but ensure that you do not give "Visitor" groups access to FOUO information.

Attachment 3

UNIT SITE OWNER APPOINTMENT TEMPLATE

Figure A3.1. Unit Site Owner Appointment Template

Note: Place the below information on appropriate letterhead.

Date

MEMORANDUM FOR 6 CS/SCXKM (SharePoint® Admin)

FROM: Unit/CC

SUBJECT: Unit Site Owner Appointment

Reference(s): MACDILLAFBI 33-301, Enterprise Information Management – SharePoint®
AMC, Enterprise Information Management (EIM), Privacy Act Manual for Site Owners
AMC, Enterprise Information Management (EIM), SharePoint 2013 Training Manual for Site Owners and Users

1. The below individuals are appointed Primary and Alternate Unit Site Owners:

	Rank	Name	Office Symbol	Phone
Primary:				
Alternate(s):				

2. Appointed individuals have completed required Site Owner training as identified in MACDILLAFBI33-301. If this is their first time being appointed as a Unit Site Owner, they will contact 6 CS/SCXK (SharePoint Admin) to schedule initial training.

3. The appointed individuals are aware of their duties as identified in MACDILLAFBI 33-301 as well as protecting FOUO information from unauthorized disclosure on SharePoint®.

4. Direct questions to appointees.

FIRST MI LNAME, Rank, USAF
Commander, Unit Spelled Out