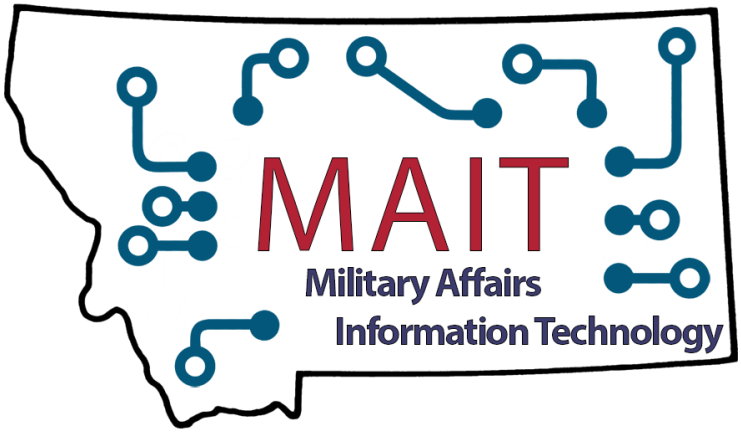
State of Montana
Department of Military Affairs

Information Technology Procedure Manual



Revised: 7/13/2021

Contents

Scope

In addition to a few special circumstances, the Department of Military Affairs Information Technology (MAIT) staff provide technical support to the following groups:

- Construction and Facilities Maintenance Office (CFMO)
- Director's Office (DO)
- Disaster and Emergency Services (DES)
- Montana Air National Guard (MANG)
- Montana Army National Guard (ARNG)
- Montana Veteran's Affairs Division (MVAD)
- Montana Youth ChalleNGe Academy (MYCA)
- STARBASE
- Training Site at Fort Harrison

This procedure manual applies to any employee or contractor (further referred to as "User") for the State of Montana Department of Military Affairs. All users shall follow these established general procedures unless otherwise stated or exempted for your organization unit in this document.

As an example, the organization unit you are assigned to will affect how you will access the various resources provided by MAIT staff (Outlook installed on your workstation vs. using the Outlook web-based application in a browser).

Agency Strategic Plan – Information Technology

In the current digital age, and more directly because of the COVID-19 pandemic, information technology infrastructure is trending toward the cloud based/remote work capability. Because of this, the Department has updated its vision to the new modern workspace . Part of this shift has been the roll out and adoption of Virtual Private Networks (VPN) across the Department, as well as implementation of Voice Over Internet Protocol (VOIP) telecommunications such as internet-based telephones and faxes.

This direction is feasible, and necessary for the success of the Department. To help with this goal, the Department will maintain an Information Technologies staff consisting of one IT Manager and three IT Technicians, two located at Fort Harrison and a technician dedicated to the MT Youth Challenge Academy located in Dillon. Technicians will be cross trained to be able to provide support throughout the Department but will also be primarily dedicated to specific projects to maintain both quality of service and infrastructure maintenance.

As much as possible while still qualifying for all security standards, cloud-based software and remote access/management programs will be implemented and utilized alongside existing systems to ensure that all users, whether they be in the office, working from home, or deployed in the field will have the ability to effectively execute their duties and missions. Also included in this pursuit is the ability to track technology assets and train users on their operation.

In addition, the IT Manager will regularly collaborate with the Division Administrators and their Bureau Chiefs to ensure that all end-user goals and needs are being met and to plan for any obstacles or opportunities for growth.

State Information Technology Services Division General Policies and Procedures

The State Information Technology Services Division (SITSD) is the governing body of Information Technology (IT) policy, procedure, and implementation for the State of Montana and its employees.

Unless otherwise referenced or declared in this document, the Montana Department of Military Affairs (DMA) has adopted the Statewide Information Technology Policies and Procedures listed in the Montana Operations Manual (MOM), which contains policies, procedures, and standards applicable to the operation of Montana state government.

DMA and its employees, and other DMA computer users are required to comply by all applicable state Legislation, Policies, Directives, Regulations, Rules, Procedures, Memoranda, and Executive Orders. Listed below is a non-comprehensive list of applicable documents which are managed by SITSD:

Legislation

1. Section 2-15-114, MCA – Security Responsibilities of Department for Data
2. Section 2-17-504 et seq., MCA – Montana Information Technology Act (MITA)
3. Section 2-17-505, MCA – Information Technology -- Internet Privacy Policy
4. Section 2-17-511, MCA – Chief Information Officer -- Duties
5. Section 2-17-512, MCA – Powers and Duties of Department
6. Section 2-17-516, MCA – Exemptions – University System – Office of Public Instruction – National Guard
7. Section 2-17-534, MCA – Security Responsibilities of Department
8. Section 5-13-309, MCA – Information from State Agencies

Policies, Directives, Regulations, Rules, Procedures, Memoranda

1. ARM Title 2 Chapter 12 Sub-chapter 206 – Establishing Policies, Standards, Procedures and Guidelines
2. ARM Title 2 Chapter 21 Sub-chapter 65 – Discipline Policy
3. NIST 800-53 – Security and Privacy Controls for Information Systems and Organizations
4. State of Montana Office of the Governor Executive Order No. 09-2016 – Implementing the State IT Convergence Plan
5. Statewide Policies: MOM
    i. Action and Exception Request Procedure
    ii. Data Classification Policy
    iii. Ethics Policy
    iv. Information Security Policy
    v. Information Security Policy – Appendix A

SITSD Policy Related Contact Information

MOM.mt.gov
406.444.2000
MOM@mt.gov

Requesting Assistance

DMA employs a staff of dedicated information technology professionals at the Help Desk available to assist users with any technical related needs or issues that may arise.

Any technical questions or inquiries should be directed to the main IT Help Desk using one of the following methods as this will allow the IT staff to provide faster support:

Help Desk Hotline

406.324.3337

Email

DMAHelp@mt.gov

Something's Broken Website Form

https://montana.servicenowservices.com/sp?id=sc_cat_item&sys_id=b1a4f2301bc5a8100b73a8efe54bcb59

In-Person Support

The MAIT room is located in Room 115 of the Fort Harrison, MT HAFRC building. Users should attempt to contact the MAIT Help Desk staff via the Help Desk Hotline, emailing the help desk or submitting a help ticket on Service Now, before visiting the IT room in person.

Office and Help Desk Hours

Monday through Friday
8:00PM – 5:00PM
Except Holidays

Users should contact the MAIT Help Desk first before reaching out for assistance from either a specific staff member or State ITSD. MYCA staff can directly contact their dedicated IT staff member located in Dillon, MT, or via the MAIT Help Desk contact info above. All MAIT staff can assist with most issues and will delegate assistance as necessary.

Setting Up A New User

Notifying MAIT Staff of the New Hire

MAIT staff will be notified of any new users for the department via the FIM Human Resources (HR) User Process. This process is initiated by the DMA Human Resources staff and automatically generates the required information for user account creation.

MAIT will be unable to assign user access, permissions, or licensing until this process has completed. Managers are still invited to send a preliminary list of access or permissions to the Help Desk to facilitate the process, however until the completion of the FIM HR New User Process access will be limited.

Account Creation

FIM will automatically create user accounts in the State.mt.ads Active Directory, which will assign attributes such as the Username and EmployeeID. MAIT will delegate the appropriate access after the automatic process completes.

Unless previously contacted, MAIT will contact the new user's manager to request a listing of required access.

For the following groups, MAIT will also have to create a user account for the user in their separate organizational unit's environment, as the user account in State.mt.ads will not be used to sign into a State.mt.ads Active Directory linked workstation:

- CFMO
- MANG
- ARNG
- MVAD
- MYCA
- STARBASE
- Training Site

These groups will maintain at least 2 login credentials, with one allowing them to sign into their dedicated workstation and the other giving them access to things like SABHRS, State webmail, and licensing. Both login credentials should have the same username, however the passwords are not linked and may be different. It is up to the user to coordinate syncing these passwords if they so choose to.

After all requested accounts are created successfully, MAIT staff will contact the user and/or their manager to provide the new login credentials.

RSA Tokens

The State of Montana utilizes a system called RSA for two-factor authentication against the State.mt.ads active directory domain. All users will need either a physical or digital token from the MAIT staff to access SABHRS and State email accounts.

Depending on your organization unit, some users may also need to use the RSA token to log into their workstations.

Licensing

The user's manger will provide MAIT will a list of the appropriate licensing and software needs for the user.

Email Account Creation

If an email account is required for the user, MAIT will create the mailbox for the user. The email address is automatically assigned by the system; however, the user does have some limited ability to request a specific address. The general scheme for new State email address is: Firstname.Lastname@mt.gov.

Federal Systems Access

MAIT does not have the ability to add, modify, or remove permissions for any system owned or controlled by the Federal government. Users for these systems must contact the Federal IT group assigned to their organizational unit, or contact the J6 Help Desk at Fort Harrison at 406.324.3160.

Access and Permissions

MAIT staff function as the gatekeepers for access to most DMA data.

At new user account creation, the user's manager will provide MAIT a list of the required access for shared drives, emails, and agency security access for the new user.

If at any time access or permissions need to be modified, the user or their manager can submit the request to the MAIT Help Desk. Any changes will require the approval of the user's manager before taking effect.

If at any time MAIT believes a user's account has been compromised, MAIT will restrict or revoke access to the affected systems until the issue can be addressed. All changes will be logged in the MAIT Help Desk.

Some organization units may require access to systems that MAIT staff do not control. In these instances, the user's manager will assist the user in contacting the appropriate governing agency or body to provide that access to the user. A non-comprehensive listing of some systems that are utilized by DMA users but are not controlled by MAIT are:

- Other agency's shared drives
- Other agency's mailing lists
- VetraSpec
- BOSS
- Federal email, Federal Microsoft Teams, Army 365, and Federal Zoom
- Other systems controlled by the Federal government

Auditing

DMA computer users must be aware of the acknowledgement statement when signing into their computer and cooperate with system administrator requests for information about computing activities. Users must follow agency procedures and guidelines to maintain a secure, virus-free computing environment, and follow agency procedures and guidelines for backing up data and making sure that critical data is saved to an appropriate location. All system activity is subject to review.

Backing Up Data

DMA users should back up all State of Montana data to a secondary source as frequently as possible. Users that do not back up data from their physical workstations run the risk of the potential complete loss of all data on the device should something go awry.

All domain-linked workstations will have a list of Shared Drives that users should copy any local data to. This list of drives will include a personal drive (generally the Y: drive) that is dedicated specifically for that individual user's private use.

Users that have been assigned a license for Microsoft Office 365 will have access to the Microsoft OneDrive service. This will back up data on a cloud server for access remotely anywhere without the need to be connected to the domain.

Data that should be backed up on a regular basis includes but is not limited to:

- Documents (.doc, .xls, .pdf, etc.)
- Pictures (work related pictures only)
- Desktop items
- Outlook .pst files
  Please note: while .pst files are allowed for some users in DMA, these files do not back up automatically. Users will manually need to back up any .pst files to a backup directory. It is strongly advised to copy emails and data from these files and upload them into the Personal Archive in your state-owned email account.

In the event of data loss MAIT will run recovery attempts on the workstation to recover data off the device, but there is no guarantee that data can be recovered 100% of the time. Any loss of state-owned data from a user's workstation due to negligence (be that direct damage or failure to maintain data backups) is subject to the State of Montana and/or DMA disciplinary policies.

MAIT is not responsible for backing up any user's local or personal data.

How to Back Up Your Data

1. Determine what data you are going to back up (individual documents, files, or entire folder structures.
2. Choose the backup location. The suggested location would be to a networked shared drive or your personal Y: drive, as these locations are backed up to a failsafe location daily by MAIT.
3. Copy or move the data. This can be accomplished by clicking and dragging the items into the backup folder, or by using the built-in copy/paste features.
4. Verify the existence of the backed-up files in the backup location.
5. Optional: If the data was sensitive or confidential in nature and you no longer need immediate access to it, you should also delete the data from your computer after the backup is complete.

Upon request, MAIT can provide a data backup script that would automate most of this process for the user. However, running the process is still the user's responsibility.

Compliance Violations

Any violation of established State or DMA procedures or policies, whether listed herein or elsewhere, is subject to disciplinary action as determined by the user's manager and/or DMA Human Resources staff.

In the event of a breach or compromise in data integrity or security, MAIT can suspend or restrict access for a user at its sole discretion in accordance with established SITSD policies.

Confidential Information

DMA users and systems must comply with the data security standards and procedures established by the Department of Administration Risk Management and Tort Defense Division (RMTD) as allowed by §2-9-101, MCA et al – Liability Exposure and Insurance Coverage.

Definition and Examples

While performing their duties, DMA users may have access to or gain knowledge of confidential information. "Confidential information" is defined as information to which the public does not have general access or is sensitive in nature.

Examples of confidential information include:

- passwords
- name, date of birth, age, sex, and address
- Social Security numbers
- current contact details of family
- banking or financial details
- medical history or records
- personal care issues
- service records and file progress notes
- veteran or disability status
- employee records
- assessments or reports

DMA users may reference the SITSD MOM-POL-Data Classification Policy for definitions and examples of how to better handle, secure, access, and use data.

Users must also abide by the State Ethics Policy when conducting business on behalf of DMA with regards to confidential information and data.

Failure to properly secure or maintain DMA data may be subject to applicable disciplinary action.

Storage of Confidential Information and Sensitive Data

As much as possible, users should utilize the provided shared drives for the storage of data and limit the amount of information kept on their personal desktops. Confidential data should be moved to shared drives or another secure location when it is no longer needed on the local workstation environment.

To permanently delete sensitive data, users can select the files and use the SHIFT+Delete Windows shortcut combination. This will also bypass the Recycle Bin and files will not be recoverable.

Cyber/Data Security Information Breaches

In the event of a suspected data breach, DMA users must immediately inform their supervisor and the Agency Security Officer/IT Manager who would investigate to determine the scope of the breach if one occurred. A Report of Incident will also be filed with RMTD.

More information, training, policies, procedures, and forms can be found on RMTD's website at https://rmtd.mt.gov/.

Cyber Security and Awareness Training

The State of Montana and the Federal government both offer cyber security and awareness trainings annually for all users free of charge.

All DMA users that access State or Federal networks are required to complete one (1) of the offered cyber security and awareness trainings annually to be eligible to access State networks and resources.

DMA Users on State Systems

DMA users that access State of Montana owned and managed systems must complete the annual cyber security and awareness training offered by SITSD.

DMA Users on Federal Systems

DMA users that access Federal government owned and managed systems must complete the cyber security and awareness training offered by the Federal government. These users will not have to take the SITSD offered training.

DMA Users on DMA Systems (Non-State or Federal)

The IT manager will work with these DMA user's Division Administrator to determine which training will best complete the requirement for training. These users will be provided information on how to accomplish this requirement after it is determined.

Exemptions

DMA users that have completed a reasonable equivalent to the offered cyber security and awareness trainings may qualify for an exemption from taking them. These users must request an exemption through their supervisor with the Information Security Officer/IT Manager and provide documentation or a certificate attesting the user has completed an equivalent training.

DMA users that fail to pass or participate in an eligible training, or the reasonable equivalent, risk having access to DMA managed networks and systems restricted or terminated until the successful completion of training at the discretion of the agency Information Security Officer in coordination with the user's supervisor.

Damage, Theft, Misplacement, and Replacement of Equipment

Unless otherwise arranged, the general duration of the device replacement cycle for DMA is 5 years. This includes workstations/laptops, company owned cell phones, RSA tokens, and peripherals.

Users must treat all state-owned equipment with care and proper maintenance. Users should not subject their equipment to harsh elements or conditions. Some examples are:

- Leaving it in the car during excessively hot or cold conditions
- Spills
- Drops
- Applying too much pressure or weight
- Not utilizing appropriate padding or protection during travel
- Misplacement, careless or negligence resulting in lost or stolen equipment.

If state-owned equipment becomes lost, stolen, damaged, or destroyed in any way, the user is required to submit a Help Desk ticket informing MAIT of the incident.

MAIT will work with the user's manager to schedule repair or replacement of the equipment as appropriate.

RSA Tokens

Physical/hardware RSA tokens all have an expiration date inscribed on the back of the unit. If the token becomes inoperable, MAIT will determine the expiration date and replace the unit if it is determined the battery is faulty.

Lost or damaged tokens will be replaced one time per user at no cost. If the user loses or damages subsequent tokens, they are liable for the cost of the replacement token.

As of 7/13/2021, the current replacement cost is $50.00 per physical hardware RSA token.

Workstations, Mobile Devices, Peripherals

Damage to a state-owned workstation, mobile device, peripheral (keyboard, mouse, printer, webcam, etc.) caused by negligence of the user may be subject to disciplinary action in accordance with established policies.

In the event of repeated damage to a user's state equipment, the user may be liable for a portion or the entirety of the replacement cost of the equipment at the discretion of the IT Manager, DMA HR, and the user's manager.

MAIT is not responsible for repairing equipment damaged by negligence or abuse unless arranged with the user and their manager. Any replacement or repair costs must be pre-approved, and a funding source determined before proceeding.

Theft or Misplacement of Equipment

Employees must immediately report a suspected theft or misplacement to:

- Their supervisor, or
- The person designated by the division administrator to research suspicious activity, or
- A management level above the employee's supervisor, or
- The IT Manager.

Reporting individuals must assure that the report is received by a member of department management. If the member of department management is unavailable, reporting individuals must report to another individual in the management structure.

The member of department management receiving the report of theft or misplacement must research to determine whether the information may be Protected Health Information and promptly report the loss to:

- Their Division Administrator and/or
- The Division Administrator of the division owning the property, and
- The IT Manager, and
- The Department of Administration Risk Management and Tort Defense Division, via completion of the "Report of Incident" form available at: http://rmtd.mt.gov/claims/agenicesreportclaims. **If the value of the loss is greater than $5000 the report MUST be made via immediate phone contact**.

The member of department management may need to report the loss to:

- Law Enforcement (if appropriate)
- If law enforcement is notified, then the Public Affairs Officer must also be notified.

If the theft or misplacement involves potentially sensitive information or Protected Health Information the same member of department management must report the loss to:

- The IT Manager, and
- The HR Manager

The IT Manager must report the theft or misplacement to:

- The Office of Cyber Protection, Department of Administration, Information Technology Services Division, and
- The HR Manager, and
- The Public Affairs Officer and
- The Department Director

In the case of any actual or suspected theft must immediately upon discovery notify both the Attorney General and the Legislative Auditor in writing per MCA 5-13-309 (3).

Email

The State provided email system is to be used for:

- the conduct of state and local government business and delivery of government services;
- transmitting and sharing of information among governmental, research, and educational organizations;
- supporting open research and education in and between national and international research and instructional institutions;
- communicating and exchanging professional information;
- encouraging debate of issues in a specific field of expertise;
- applying for or administering grants or contracts;
- announcing requests for proposals and bids;
- announcing new services for use in research or instruction; and
- conducting other appropriate State business.

All emails created, sent, or received, over the State email system are the property of the State of Montana. Except as provided by law; emails created, sent, or received over the State email system may be public information. Employees should not have expectations of privacy for any emails. Department system administrators and management, and Department of Administration personnel, may monitor email for performance, troubleshooting purposes, or if abuses are suspected.

Access to the State email system may be restricted by the Department without prior notice and without the consent of the user. Any employee who abuses the privilege of email may be subject to disciplinary action up to and including termination of his or her employment. The Department may inform appropriate legal officials, including law enforcement personnel, of any email abuses.

The Department recognizes that use of the State email system for personal/non-business reasons may occasionally be necessary and may be more efficient than using the telephone or leaving the office to conduct personal business. At the same time, the public has a right to expect that government resources such as the State email system are used primarily for government business. Thus, use of the State email system for personal/non-business reasons must be kept to a minimum.

Email users are required to use a more secure means of transmission such as the ePass file transfer service, https://transfer.mt.gov , when communicating Federal Tax Information (FTI), sensitive Personally Identifiable Information (PII), or Protected Health Information (PHI). Note that more than one piece of non-sensitive PII for one individual in the same message can result in sensitive and private information in the aggregate, and should be avoided or sent by secure means.

Types of Email Accounts

DMA utilizes the following email account types:

1. User Mailbox
2. Resource Mailbox (Room, Equipment, or Shared)

All users that are considered Normal Users or Contractors/Contingent Workers are eligible for a State of Montana @mt.gov email address for business use through their included Microsoft Office 365 licensing. These users are assigned the “doaITSDBillingCode” attribute “0” or “10”.

HR Self Service Users and Limited Contractors/Limited Contingent Workers are not assigned licensing for Office 365 applications and are restricted to SABHRS access only.
These users are assigned the "doaITSDBillingCode" attributes "2" or "15".

Email Account Creation

After the users new account is created in the State.mt.ads Active Directory following the automated FIM HR New User process, MAIT will be able to create the user's @mt.gov email address by using the SITSD Exchange Tasks portal.

As of 7/13/2021, all new State emails will use the following address scheme:

Firstname.Lastname@mt.gov

Users may request a different new email address by submitting a Help Desk ticket.

Accessing State Email

Users may access their state email using one of the following methods:

- Outlook application installed on your workstation (only available to State.mt.ads joined workstations, currently DO, DES, and TAG office).
- Webmail/Outlook.com
- Mobile application on mobile device

Outlook Application

Users should be able to open the Outlook application after the first log in with the embedded domain credentials inherited from the server and minimal prompting.

Webmail/Outlook.com

All users can access their state email via a web browser using the following steps:

1. Navigate to the new Webmail portal by opening a web browser (preferably Google Chrome or Edge) and going to Outlook.com. You will be redirected to outlook.live.com/owa
2. Click the "Sign in" button in the top right corner.
3. Enter your State of Montana email address (i.e., YourEmailAddress@mt.gov) and click Next.
4. Enter your CW# and Email/SABHRS password, then click "Sign in". Delete everything except your CW#, including @mt.gov if pre-populated.
5. Enter the passcode from your RSA Token, then click "Submit".
6. If this page is displayed, you can click "Yes" to stay signed in. This will reduce the number of times you are asked to enter your password. If you are not using your issued workstation, you MUST sign out after each session or you will stay signed in.

Mobile Applications on Mobile Devices

If you would like to add your state email on your mobile device, please contact the MAIT help desk for current instructions on getting set up.

Sharing Office 365 Folders (Mail, Calendar, Contacts) With Another User

As of February 1, 2021, SITSD and MAIT are longer managing permissions for shared mailboxes and calendars. End users should manage permissions themselves using the tools built into the email system.

If you would like to give a person permission to access a folder in your Office 365 account, it involves giving permission in **two** places. First, you need to give the person permission to access your Office 365 e-mail account Mailbox (e.g., Mailbox - Doe, Jane) then you need to give the person permission to access each Folder/Subfolder you want to share. The process for sharing your Mailbox and your Individual folders is the same.

Sharing your folders using Outlook

1. Right-click on your Mailbox name (e.g., Mailbox-Doe, Jane) and select **Folder Permissions**.
2. Select the **Add** button.
3. Select the person you wish to give permission to from the address list and press the **Add** button.
4. Press the **OK** button.
5. Click on the person's name and select the appropriate permissions from 'Permission Level:' drop down list (e.g., Owner, Contributor...). Reviewer rights are recommended at the Mailbox level. The option "Folder Visible" must be selected.
6. Click the **OK** button.

Now you will need to give permissions to the actual mail folder, subcalendar or contacts.

1. Right click on the folder you wish to share (if wanting to share a subcalendar or contacts, you will need to click the **... icon** and choose **Folders icon** to view all folders)
2. Select **Properties or Sharing Permissions** (depending on your Outlook version) and click **Permissions** tab.
3. Click the **Add** button.
4. Select the person you wish to give permission to from the address list and press the **Add** button.
5. Press the **OK** button.
6. Click on the person's name and select the appropriate permissions from 'Permission Level:' drop down list (e.g., Owner, Contributor...).
7. Click the **OK** button.
8. To share additional folders/subfolders, right-click on the folder or subfolder you wish to share and follow steps 2-7 above.

Accessing another person's folder(s) using Outlook

To open another person’s folder(s), you need to make sure that you have been given permission to their Mailbox account and the Folders/Subfolders in that Mailbox account that you wish to access (e.g., See steps 1-7 above). Then proceed with Step 1 below.

1. Choose **File | Account Settings**.
2. Select your **Office 365 account** and click the **Change** button.
3. Click the **More Settings** button.
4. Click the **Advanced** button.
5. Under Mailboxes, 'Open these additional mailboxes:' click on the **Add** button and type the person's name in the window (e.g., Jane Doe), and click the **OK** button.
6. Click the **OK** button.
7. Click the **Next** button.

8. Click the **Finish** button.
9. Restart **Outlook**.

The folder will appear at the bottom of your folder list.

Sharing your folders using OWA

1. Login to OWA
2. Choose **Mail** to open your Mail folders.
3. Right click on your name in the Mailbox list
4. Select **Permissions**
5. Click the **+** button to add a new person
6. Type the name of the person you are sharing the folder with and click **Add**
7. Select the desired permission level (Reviewer is recommended) - Folder visible must be a selected option.
8. Click **OK**

Now you will need to give permissions to the actual mail folder, subcalendar or contacts.

1. Right click the folder you wish to share and select **Permissions**.
2. Click the **+** icon and type the name of the person you are sharing the folder with and click **Add**
3. Select the desired permission level
4. Click **OK**
5. Repeat steps 2-7 for the folder(s) you wish to share.

Accessing another person's folder(s) using OWA

1. Login to OWA
2. Click **Mail** to open your mail folders.
3. Right click on your name in the folder list.
4. Choose **Add Shared Folder**
5. Type the name of the person whose folder you wish to open and click **Add**
6. The folder will appear at the bottom of your folder list.

File Sharing

Files in the DMA environment may be stored or saved in several ways:

- Locally on the workstation (desktop, documents folder, user folders, synced folders, etc.);
- On networked shared drives;
- On Microsoft Office OneDrive;
- File Transfer Service
- On DMA issued storage drives (flash drives, external hard drives, SD cards, etc.);
- On mobile devices (both DMA issued and personal devices accessing DMA data).

It is the responsible of the user to maintain the integrity and security of their files and data, and to ensure that data is properly stored and backed up regularly.

Locally/Saved on the Workstation

- Data saved locally on the user's workstation does not get backed up or stored elsewhere.
- Data saved locally is not available to any other user or person.
- This data is the user's sole responsibility.
- Data saved locally should be migrated to another source (shared drive, OneDrive) when it is no longer actively being used to prevent data loss.
- MAIT staff may be able to attempt to recover lost data but cannot guarantee its retrieval.

Networked Shared Drives

- Data saved on networked shared drives gets backed up regularly by MAIT staff via automated processes.
- Data saved on networked shared drives is available to other users that have been granted access to that file or folder location.
- Access to networked shared drives is managed and controlled by MAIT. Access is determined based on job duties.
- Modifications to networked shared drives access can be requested by submitting a help desk ticket and requires supervisor approval.

Microsoft Office OneDrive

- Data uploaded to OneDrive is encrypted and stored via the cloud on Microsoft Servers.
- Data saved on OneDrive can be shared or access granted/revoked by the user via the built in "Share with" tool.
- MAIT does not have the ability to modify access or permissions to OneDrive.
- OneDrive is auditable via SITSD if a discovery request is made through SITSD internal processes.

File Transfer Service

- State of Montana employees and public citizens can utilize the File Transfer Service (FTS) to send documents to anyone with an ePass account (free to create for all users, including the general public).
- FTS is encrypted and private.
- Confidential and sensitive information can be transmitted via FTS due to its integrated security, monitoring, and virus scanning features.

- Data is stored for a temporary time frame before being deleted automatically from the system.

DMA Issued Storage Drives

- Data should only be saved to storage drives temporarily when transporting it between locations or for presentations on other workstations.
- Data saved on storage drives is not available to any other user or person.
- This data is the user's sole responsibility.
- MAIT staff may be able to attempt to recover lost data but cannot guarantee its retrieval.
- Because of the mobile nature of these drives, they should not be used for storing or transporting confidential or sensitive information.

Mobile Devices

- Includes both DMA issued and personal devices owned by the user.
- Documents and confidential or sensitive data should never be stored on a mobile device.
- Use should be restricted to email or calendar data, unless explicit permission is granted from the user's supervisor or the IT Manager.
- Lost data is unrecoverable.
- DMA approved applications are allowed (Outlook Mobile, Microsoft Authenticator, RSA Authenticator, Intermedia Unite, TeamViewer).

Exceptions have been granted to the MYCA and STARBASE programs that use mobile devices, tablets, iPads, and laptops for educational use related to the scope of their programs.

Guest/Visitor Use of Workstations and Licensing

DMA users are not permitted to allow guests, visitors, or family members to access or use a DMA owned workstation unless conducting business on the behalf of the State of Montana pursuant to MCA § 45-6-311. Unlawful Use of a Computer.

Shared Workstations

Some workstations are provided for group functions, like conference rooms and meetings, and have been set up with local generic user accounts for DMA related business. Users are not permitted to utilize these accounts for personal use or allow any other person to use them for non-DMA related use.

State-issued Software Licensing

The State of Montana software licensing for some products does allow for users to install software products on personal devices (i.e., Microsoft Office products). While users may utilize these products on personal equipment, they must maintain a valid license seat on their DMA issued workstations at all times.

In the event of a shared personal device (i.e., a family computer or mobile phone), DMA users must sign out of their State of Montana accounts when not conducting DMA business to preserve data integrity and prevent unauthorized use. Failure to do so may result in disciplinary action.

Network Access

All network access is controlled and monitored by MAIT and SITSD network security.

Physical Network Access (LAN)

Physical network access is the easiest way for bad actors to gain access to sensitive information and perform attacks on department infrastructure.

DMA Users should not connect any device to the network that was not issued by MAIT staff or cleared for use by SITSD network security.

DMA issued workstations and other devices have been preconfigured for access to the physical network.

Wireless Network Access (WLAN)

MAIT provides DMA users with multiple wireless networks at all office sites to allow employees and visitors access to the internet with compatible devices.

Any person connecting to the WLAN should only connect to the Network Service Set Identifier (SSID, or the "network name" i.e. DMA-Guest or DMA-Secure) appropriate for the intended use.

Secure Wireless Networks

Several secure wireless networks are provided for State of Montana employee use only. Users connecting to these networks are only allowed to connect with State or DMA issued devices.

Any user connecting to a secure wireless network with an unauthorized device will have their network access revoked.

Examples of the secure wireless networks utilized by DMA and the State of Montana are:

- **MontanaSecure**
  - For users connected to the State of Montana SITSD SummitNet network. This primarily applies to users with DES, the Director's Office, and other State of Montana agencies. This network is also available in other State-owned buildings and is managed by SITSD.
- **DMA-Secure**
  - For users connected to the SECC, MVAD, MYCA, CFMO, and STARBASE networks.
- ***Please note:*** **DMANETWORK** is in the process of being phased out. If your office still has access to DMANETWORK, please contact the MAIT Help Desk prior to connecting any device to the wireless network.

Guest Wireless Networks

MAIT provides DMA users and visitors with access to the public guest networks. These networks do not have server or network drive access and are to be used for all unsecured or personal devices.

Examples of the available guest networks provided by MAIT are:

- **DMA-Guest**

Passwords

DMA users must follow the password policies and guidelines established by SITSD for all business-related accounts and services.

Password Requirements

- 14 characters or more
- At least 1 number
- At least 1 Uppercase and 1 Lowercase letter
- At least 1 special character

Account Lockouts

- 6 incorrect password attempts will trigger an account lockout
- Accounts will automatically unlock after 15 minutes
- Contact MAIT if you need access immediately

Password Security

Users should not store passwords in an easily accessible location (i.e., post-it notes, notepads, stickers, etc.).

Users should not share their password with any other user, except for MAIT staff in the process of assisting the user with an incident. If sharing a password is intended to grant a user access to a shared system, the user should instead submit a Help Desk ticket to grant appropriate privileges and to maintain system security protocols.

Remember Me Checkboxes

Unless otherwise instructed by MAIT or the Agency Security Officer, users should refrain from checking any box that would allow a system to remember the user's password for them.

> *MS Office 365, Office.com, Outlook.com, and State webmail have been granted an exception.*

Personal Technology/Bring Your Own Device

DMA does allow some users to utilize personal equipment when conducting DMA business. All personal equipment intended to be used to conduct DMA business must first be determined to be appropriate and necessary to fulfill a job-related function by the user's supervisor, then approved by the user's supervisor and the IT Manager. The IT Manager maintains authority over granting requests for such situations and may deny or revoke related requests or permissions at any time at their discretion.

Unless necessary, DMA should work with the user to provide the equipment necessary to perform required job functions.

Mobile Phones

DMA will provide users a state-issued mobile device if it is necessary to perform critical job duties. The user's supervisor in coordination with MAIT staff will determine the device and cellular plan necessary for the requested functions.

All users in DO/MVAD/MYCA can answer calls made to their desk phones on their workstations by utilizing the VOIP phone system companion application (Currently Intermedia Unite).

DMA does provide mobile device use reimbursements to eligible users pursuant to the DMA Cellular Device Use and Reimbursement Policy. Users should seek permission from their supervisor before submitting the Employee-Owned Cellular Device Reimbursement Authorization Form for signature and approval by their supervisor, the Division Administrator, and the IT Manager.

Workstations/Laptops/Desktops

DMA is currently decommissioning all provided desktop and stationary workstations (except for shared workstations) for users in favor of laptops and tablets. All users who work remotely should speak to their supervisor about being assigned a laptop or tablet.

The IT Manager may grant written exceptions to this standard if a reasonable need exists.

Users may not need to be issued a workstation at the discretion of their supervisor and depending on their role and job duties. Users do not need to be issued a workstation for accessing SABHRS or Office365/Google Enterprise web-based applications.

Peripherals (keyboards, mice, monitors, printers, etc.)

Users should refrain from using personal peripherals connecting to DMA equipment unless authorized by MAIT staff. Users needing additional equipment for job related functions should submit a help desk ticket for the request.

Users may not at any time install software for personal devices without requesting help from the help desk.

MAIT staff may request the removal or discontinuation of any personal peripheral if it is found to be in violation of policy or poses a threat to the workstation or network.

Connecting to State Resources

Users may not at any time use a personal device to connect to or access DMA business related resources unless they have been granted written permission from their supervisor and the IT Manager.

Personal Use of State-Owned Equipment

DMA staff can use state-owned equipment in reasonable amounts insofar as personal use is not excessive or disrupts the user's ability to execute their job duties.

A reasonable amount is generally defined as between 2% - 3% of a workday, or between 10-15 minutes each day for a full-time employee. This is subject to further restriction as deemed appropriate or necessary by the user's supervisor.

Streaming Services

Users are not permitted to use or install any software or services on state-owned equipment that stream or provide a constant feed of data that would be considered personal use.

This includes, but is not limited to:

- Audio (music, audio books, talk shows and radio, etc.)
    - *Examples: Spotify, Apple Music, YouTube Music, Tidal*
- Video (movies, films, television shows, etc.)
    - *Examples: Netflix, Hulu, Amazon Prime Video, YouTube, Disney+, Twitch*
- News Media
    - *Examples: ABC, CBS, CNN, Fox News, MSNBC, NBC*

Wireless Internet

DMA staff can connect to DMA provided wireless networks using personal devices so long as the use is not excessive or disrupts/reduces the ability for business to be conducted.

Users should not access Streaming Services from their personal devices while connected to DMA provided wireless networks.

Excessive Use or Unauthorized Access

Users that are determined to be using state-owned equipment, including wireless internet, excessively may be subject to disciplinary action in accordance with State of Montana policies.

Users that are found to be accessing restricted resources or services using state equipment may be restricted or disconnected from the network.

Users using a personal device to connect to state-owned equipment, including wireless internet, in an excessive or inappropriate manner, may be blocked from using the network or resource at the discretion of the Information Security Officer/IT Manager.

Purchasing

DMA will provide users with the workstations, peripherals, software, and hardware necessary for them to effectively execute their duties.

It is the responsibility of the user to work with their supervisor to determine the equipment necessary to perform job related duties.

MAIT staff will utilize the help desk system to track and process information technology related purchases.

Purchasing and Procurement Process

1. The user will coordinate with their supervisor to determine the scope or need related to any information technology related purchase.
2. The user will submit a help desk ticket to the MAIT staff with the details of the request.
    a. MAIT staff will help the user determine the appropriate equipment or software necessary to fulfill the needs of the user, which may include additional research or suggestions for compatibility.
3. MAIT staff will coordinate with the user, their supervisor, and if necessary the designated financial officer of the funding source to determine method of payment.
    a. If MAIT staff will process the purchase:
        i. IT Manager will provide a quote in writing for the proposed purchase with all applicable details to the user and their supervisor;
        ii. A DMA user with authority for the funding source will review and approve the quote in writing;
        iii. IT Manager will proceed with the purchase and provide an order confirmation or invoice to the user and their supervisor;
            1. If the order requires additional verification or authorization in accordance with State of Montana procurement and purchasing procedures, the IT Manager will follow the associated procedures;
        iv. If the item is shipped to MAIT, they will receive the item and provide it for the user in working condition.
    b. If the user will process the purchase:
        i. User will provide a quote in writing to the IT Manager for approval.
        ii. IT Manager will review and provide approval for the purchase in writing.
        iii. User can proceed with the purchase in accordance with their funding source's established procurement and purchasing procedures.
            1. If the order requires additional verification or authorization in accordance with State of Montana procurement and purchasing procedures, the IT Manager will follow the associated procedures;

In all cases, DMA users and employees must follow all applicable State of Montana purchasing and procurement procedures as established by the State of Montana State Procurement Bureau and SITSD.

More information is available on their websites located at https://spb.mt.gov/ and https://sitsd.mt.gov/Vendors/Technology-Acquisitions.

Records Retention

DMA is required to abide by the records retention policies and schedules established by the Montana Secretary of State's office (SOS).

The Secretary of State's office maintains an up-to-date listing of all policies, procedures, forms, and schedules on their official website located at https://sosmt.gov/Records/State/.

General Records Retention Schedules

The following schedules are listed on the SOS website:

GS1	SABHRS Financials
GS2	General Financial Records
GS3	Administrative and Legal Records
GS4	Purchasing and Procurement Records
GS5	Payroll and Personnel Records
GS6	Technology Services Records
GS7	Records Management
GS8	Licensing
GS9	Non-record Material

Security Systems and Safeguards

DMA may utilize a variety of security and safeguard systems that are intended to protect user and customer data, prevent unauthorized access, and monitor or record public areas and lobbies to ensure the safety of our staff.

Some of these systems include but are not limited to:

- Network firewalls
- Camera and video recording systems
- Digital door locks
- Motion sensors
- Panic buttons
- Security systems and alarms

Installation and use, or potential removal, of these systems is based on eligible criteria to be determined by the supervisor or supervisory staff of the affected users or area in conjunction with the IT Manager, or to maintain compliance with SITSD, State, and Federal policy and law.

DMA users are prohibited from tampering with or disabling DMA security systems or safeguards. Only MAIT staff, or pre-approved delegates, are permitted to install, access, modify, or remove these systems.

Access to data gathered by these systems is granted based on compliance with applicable departmental investigations, law enforcement requests, and network security operations.

Unacceptable Use

All users are encouraged to practice ethical decision making and follow all State of Montana rules and regulations when accessing or utilizing DMA systems.

Use of any DMA system, network, or resource is subject to the following guidelines:

1) DMA owned systems and networks may not be used directly or indirectly by any user for the download, creation, manipulation, transmission, or storage of:
   a) Any offensive, obscene, or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
   b) Unlawful material or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalize themselves or others;
   c) Unsolicited "nuisance" emails;
   d) Material which is subsequently used to facilitate harassment, bullying and/or victimization of a member of DMA or a third party;
   e) Material which promotes discrimination based on race, gender, religion or belief, disability, age or sexual orientation;
   f) Material with the intent to defraud or which is likely to deceive a third party;
   g) Material which advocates or promotes any unlawful act;
   h) Material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or
   i) Material that brings DMA into disrepute.
2) DMA systems and networks must not be deliberately used by a user for activities having, or likely to have, any of the following characteristics:
   a) Intentionally wasting staff effort or other DMA resources;
   b) Corrupting, altering, or destroying another User's data without their consent;
   c) Disrupting the work of other Users or the correct functioning of the DMA network; or
   d) Denying access to the DMA network and its services to other users.
   e) Pursuance of commercial activities (even if in support of DMA business), subject to a range of exceptions.
3) Any breach of industry good practice that is likely to damage the reputation of DMA systems will also be regarded prima facie as unacceptable use of DMA systems.
4) Where DMA system are being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of DMA assets.
5) Users shall not:
   a) Introduce data-interception, password-detecting or similar software or devices to DMA's network;
   b) Seek to gain unauthorized access to restricted areas of DMA's network;
   c) Access or try to access data where the user knows or ought to know that they should have no access;
   d) Carry out any hacking activities; or
   e) Intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software.

VPN and Remote Access

MAIT staff will provide all eligible users working remotely with the ability to access DMA resources from their alternate work location.

Alternate work locations my include but are not limited to:

- The user's residence;
- Temporary lodging;
- Commercial establishments;
- Temporary or mobile networks (hotspots, JetPacks, wireless access points, etc.)

All users will coordinate with their supervisor to determine if they are authorized to work remotely. MAIT staff are not responsible for making that determination but are able to provide advice for individual situations.

DMA will not be responsible for providing internet or telecom services, including technical support for those services, to alternate work locations.

VPN

DMA will provide eligible employees with the ability to use a Virtual Private Network (VPN). VPN is a method employing encryption to provide secure access to a remote computer over the internet.

Depending on the user's organization unit, DMA may deploy one of several different VPN options tailored to their specific needs.

DES/DO/TAG Users

Users in the DES/DO/TAG offices are connected to the State.mt.ads domain and will be able to utilize the Cisco AnyConnect Mobility Client. This service is maintained primarily by SITSD with DMA providing desktop support for local installations on user workstations.

Any user in these networks is eligible for use of the Cisco VPN system.

Information on using Cisco AnyConnect is available on the DMA Knowledge Base located at https://dma.mt.gov/Directors-Office/IT/FAQ.

MYCA/MVAD/STARBASE Users

Users in the MYCA/MVAD/STARBASE offices are connected to the DMA private domain and will be able to utilize the Barracuda VPN Client. This service is maintained exclusively by MAIT staff.

Any user in these networks is eligible for use of the Barracuda VPN system. Users that do not have access to the VPN system will need to submit a help desk ticket and MAIT staff will assist the user with setting up their VPN profile on their workstation.

Information on using Barracuda VPN Client is available on the DMA Knowledge Base located at https://dma.mt.gov/Directors-Office/IT/FAQ.

ARNG/CFMO/MANG/Misc. Users

Users in the ARNG/CFMO/MANG/Misc. offices do not have the ability to utilize DMA managed VPN systems.

Website

The DMA websites are created and maintained with the understanding that they serve as the public "face" of the Department and may constitute an individual's first and only interaction with the Department.

Therefore, it is important that websites reflect the customer-oriented philosophy of DMA. They will be "user friendly." In other words, they will be presented in a form and format that the public can readily understand and navigate.

To accomplish this, the Websites will:

- Contain accurate and up-to-date information;
- Contain information pertinent to the public and to the mission of the Department;
- Be accessible to Internet users as mandated by state and federal laws and regulations;
- Be accessible via hand-held devices, such as smartphones and tablets.
- Be maintained as a single site with many unique parts rather than as a portal to many separate websites;
- Be organized in a way that does not require knowledge of the Department's administrative structure;
- Include an easy-to-find index of all programs and services;
- Have web page content written in concise, simple, everyday language;
- Avoid the use of government and professional jargon;
- Minimize the use of acronyms, and spell out at least once on each web page any acronyms that are used; and
- Provide explanatory information as needed for documents available on the site.

Accessibility

The Department's website will be accessible in compliance with Section 508 (29 U.S.C. '794 d) and meet current standards for accessibility as proscribed by rule by the US Access Board (http://www.access-board.gov).

Information on Accessibility and how to create accessible content can be found at https://mn.gov/mnit/about-mnit/accessibility.

Copyright

Copyrighted material must not be posted on the website unless express permission of the author has been obtained. If copyrighted material is posted, describe the specific permission granted for its use. Content managers are responsible for determining and satisfying copyright or other use restrictions when publishing or otherwise distributing material found on website. As a public agency, we generally do not own rights to material on our website. Most of the material on our website consists of new or republished government documents and as such, it is considered public domain. So, we do not generally grant or deny permission to publish or otherwise distribute it.

Links, Advertising

DMA has adopted the State of Montana policy regarding advertising and links:

- DMA will not accept banner ads and vendor-hosted advertising on its website.
- DMA will not link to organization, citizen, or business websites unless one of the following conditions is met:
    - The link adds appropriate value to the DMA site, is in the agency's best interest, does not discriminate against similar sites, and is relevant in content.
    - The Department has an active contract with the organization, the link adds appropriate value to the state site, is in the state's best interest, and is relevant in content.
    - The link provides access to a website that contains software that is necessary or enhances the operation of the Department site.