National Mediation Board

Office of Information Services
(OIS)Arbitration Work Station
(AWS) User Access Request

PURPOSE:
The purpose of this User Access Request process is to provide users with the National Mediation Board's (NMB) system Rules of Behavior (ROB) and ensure system access is requested and approved through the use of the Access Request form. Instructions to fill out and route the form are located in the appendices.

The ROB defines responsibilities and procedures for the secure use of National Mediation Board equipment and information technology (IT) systems. By reading and signing the Rules of Behavior, Users (defined below) acknowledge their responsibility for complying with the ROB. You will be required to sign and acknowledge that you understand the ROB.

To obtain access to NMB's systems, an Access Request Form is provided for you or your Supervisor to fill out.

RULES OF BEHAVIOR

The Rules of Behavior apply to Users who access or maintain any National Mediation Board equipment and IT systems, regardless of location, e.g., at regular duty station, at telework, or on travel. Users are individuals who have access to National Mediation Board data, equipment, and IT systems for the purpose of performing work on behalf of the National Mediation Board. Examples of Users include, but are not limited to, National Mediation Board employees, employees of contractors, sub-contractors, and agents. At the National Mediation Board's discretion, certain individuals who have access to National Mediation Board's data, equipment, and IT systems may not be considered Users under this definition and as such may not be required to sign these Rules of Behavior. In addition to the rules and requirements contained within this document, Users should note that other federal laws and regulations apply when accessing National Mediation Board's resources (e.g., licensing agreements and copyright laws), but are considered outside the scope of this document.

USERS SHALL:

Follow these rules regarding National Mediation Board data, equipment, and IT systems:

- Use National Mediation Board data, equipment, and IT systems properly; following laws, regulations, and policies governing the use of such resources.
- Protect National Mediation Board equipment, software, and data in their possession from loss, theft, damage, and unauthorized use or disclosure.
- Secure mobile media (paper and digital) based on the sensitivity of the information contained.
- Use appropriate sensitivity markings on mobile media (paper and digital).

- Promptly report any known or suspected security breaches or threats, including lost, stolen, or improper/suspicious use of National Mediation Board data, equipment, and IT systems to the Help Desk at it@nmb.gov.
- Not attempt to circumvent any security controls.
- Logoff, lock, or secure workstation/laptop from unauthorized access to National Mediation Board IT systems or services when leaving a workstation/laptop unattended.
- Not read, alter, insert, copy, or delete any National Mediation Board data except in accordance with assigned job responsibilities, guidance, policies, or regulations. The ability to access data does not equate to authority to access data. In particular, Users must not browse or search National Mediation Board data except in the performance of authorized duties.
- Not reveal any data processed or stored by the National Mediation Board except as required by job responsibilities and within established procedures.
- Dial-in or other remote access to National Mediation Board systems is prohibited, unless specifically authorized by the National Mediation Board's Chief Information Officer (CIO) or designee.
- Not install or use unauthorized software on National Mediation Board equipment.
- Retrieve all hard copy sensitive printouts in a timely manner.
- Take reasonable precautions to prevent unauthorized individuals from viewing screen contents or printed documents.
- Not open email attachments, or click links, from unknown or suspicious sources.
- Be responsible for all activities associated with their assigned user IDs, passwords, access tokens, identification badges, Personal Identity Verification cards, or other official identification device or method used to gain access to National Mediation Board data, equipment, and IT systems.
- Use only equipment and software provided by the National Mediation Board or that has been approved for use by the National Mediation Board's CIO or designee to conduct National Mediation Board business.
- Comply with any National Mediation Board restrictions on publishing National Mediation Board information to social media and public websites.

Follow these rules regarding access credentials:

- Protect passwords from improper disclosure. Do not reveal passwords, PINs, or other access credentials. Password or PIN disclosure is considered a security violation and is to be reported as such.
- Do not share passwords with anyone else or use another person's password or other access credential such as, but not limited to, someone else's PIV card.
- Change passwords as required by expiration dates.
- Violation of these rules may be grounds for legal and/or administrative action by the National Mediation Board and may result in actions up to and including disciplinary action, termination of access, termination of employment, contract termination, and/or prosecution under federal law.

National Mediation Board

Office of Information Services
(OIS)Arbitration Work Station
(AWS) User Access Request

RULES OF BEHAVIOR ACKNOWLEDGMENT

I acknowledge that I have read, understand, and will comply with the National Mediation Board Rules of Behavior. I understand that failure to comply with the Rules of Behavior could result in verbal or written warning, removal of system access, reassignment to other duties, criminal or civil prosecution, and/or termination.

Signature:	Date:
Printed Name	Arbitrator (Yes/No) - Company

National Mediation Board

Office of Information Services (OIS)

User Access Request

User Information:	
1. Name: (Last, First, Middle Initial)	**2. Email**:
3. Type of User: (Check one) ☐ Federal Government Employee ☐ Contractor	
4. Access Type: (Check one) ☐ Standard User ☐ Privileged User	
5. System Role:	
6. System Name: **NMB APPS - AWS**	
7. User Signature:	
Date:	
8. Supervisor/ COR Approval:	
Name: (Last, First, Middle Initial) Date:	
Signature:	
9. System Owner Authorization:	
Name: (Last, First, Middle Initial) Date:	
Signature:	
10. Additional User Information:	

Appendix A

User Access Request Form Instructions

In addition to the Rules of Behavior Acknowledgement, the User Access Request Form portion must be filled out to request access to any National Mediation Board systems and applications.

1. Enter in the **name of the person** who will be requesting access to the systems.

    a. For example, if you are a supervisor filling this out for a newly hired employee, you will fill this out on behalf of the employee. The user request will then be routed to the user for signature on the Rules of Behavior section. As the supervisor, you will then be required to provide a digital signature for approval.

    b. If the employee is filling out the request for a new account or different access to a system that was not identified in the original access request, the employee will need to fill out the form completely.

2. Enter in the employee's **email address**. This information can be obtained by contacting it@nmb.gov.

3. **Type of User** will be either a Federal employee or a contractor. Check one of the boxes.

4. **Access Type** is the type of privilege that the user will need in order to accomplish their work on the systems.

    a. For example, a user account created for pulling records from a database doesn't need admin rights (privileged account), while a programmer whose main function is updating lines of legacy code doesn't need access to financial records. The programmer, if needed, would have standard rights to the financial records if their job function includes being a user.

    b. As indicated in the Rules of Behavior section titled "Follow these rules regarding National Mediation Board data, equipment, and IT systems" if your assigned job responsibility is for privilege access you will be granted authority by your Supervisor to have t read, alter, insert, copy, or delete any National Mediation Board data except in accordance with assigned job responsibilities, guidance, policies, or regulations. The ability to access data does not equate to authority to access data. In particular, Users must not browse or search National Mediation Board data except in the performance of authorized duties.

5. **System role** is also known as role-based access control (RBAC) or role- based security. RBAC

mechanisms can be used by a system administrator in enforcing a policy of separation of duties. This further defines the privilege and standard access type for systems and applications. The types of system roles could be roles based upon groups and individuals. The following are the types of system roles that could be defined at NMB:

a. Group - Office of Legal Affairs Group (OLA) – only people in this group have access to the data in their files and data.

b. Individual – DAEO has access to the data in Ethics and in a select folders of the Office of Fiscal Service (OFS). However, this individual may not have access to OIS folders as his/her role does not require access.

6. **System name** is the system that the user will need access to. For each system a separate access request form is required. An example of a system that users may need access to is Google Suite (Email, Google Drive, Calendar, etc.)

7. **User Signature** is required for requesting access.

8. **Supervisor/COR Approval** is the direct line supervisor or the Contracting Officer Representative (COR) who approves of the user having access to the system identified. This is a required approval. This will need to be routed to your supervisor/COR for signature.

9. **System Owner** approval is the person who is accountable for the system. This is the individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of an information system. Once your supervisor/COR has approved the request, the System Owner will need to approve the request.

10. **Additional User Information** is a space for any other items that may be important for the user's access Examples of these scenarios are:

    a. A user could be an Intern that only needs access for a specified period of time. This type of information would be added into this space so that the systems administrator can limit the time period of access or disable the account while the Intern is not actively working for NMB if they are attending classes and will be back during identified breaks. The account will need to be enabled during these active periods.

    b. An auditor who has a specified time period of access and the account will be disabled at a determined date.

Appendix B

Routing Instructions

Routing instructions after filling out and signing the ROB and User account request:

1. Sign the ROB and the User Access Request Form.
2. Send to the Supervisor/COR for approval. Supervisor/COR will need to return the signed document to you. Once the form is returned,
3. Send to the System Owner for approval. The System Owner will need to return the signed document to you. Once the form is returned to you,
4. Send it to it@nmb.gov for processing of the account.