



**MIAMI VALLEY EDUCATIONAL COMPUTER ASSOCIATION
REGIONAL COUNCIL OF GOVERNMENTS**

Member of the Ohio Education Computer Network
Since 1980

ACCOUNT REQUEST PACKAGE
Revised 1/2009

This package contains all the materials that you will need to request a new account or renew an existing one. Included in this package you should find the following:

- This cover/instruction sheet
- Account Policies and Procedures
- Information Technology Center information sheet
- Instruction sheet for filling out the account request form
- Account request form(s)

In order to request a new account, or renew an existing one, you need to do the following:

1. Read the Account Policies and Procedures. *Your signature on the Account Request Form indicates that you have read and agree to comply with the established policies.*
2. Fill out the Account Request Form. An instruction sheet is provided to help you do this.
3. Ensure that all necessary signatures for the “Required Signatures” box on the form have been obtained.
4. You are advised to retain a copy of your request form, please make a photocopy of it in case it gets lost in the mail.
5. Send your completed form via U.S. mail to MVECA. The address is provided on the Data Center Information Sheet.
6. An account will be created for you within five business days of the receipt of a properly filled out and signed form. Your immediate supervisor will be notified by a phone call that your account has been created and he/she will request that you contact the MVECA Data Center to receive your username and password.



Member of the Ohio Education Computer Network
Since 1980

MVECA INFORMATION TECHNOLOGY CENTER INFORMATION SHEET

Welcome to the MVECA Information Technology Center!

Your account will be created on a VMS computer system, which is physically located in the MVECA Information Technology Center at 330 East Enon Road, Yellow Springs, Ohio.

Below you will find some general information about the MVECA Information Technology Center, our hours and operational procedures.

- **Location:**

Miami Valley Educational Computer Association
330 East Enon Road
Yellow Springs, Ohio 45387

- **Support Hours:**

The Information Technology Center phone lines are answered during normal business hours (see below). The person who answers the phone will take your name, phone number and a brief description of your problem. Your call will be logged and either you will be transferred to the person who supports the kind of problem you are having or that person will return your call as soon as possible.

- **Phone Number:**

1. Normal Business Hours: The normal business hours for MVECA are from 7:30 a.m to 4:30 p.m. There are four lines available for obtaining support during these hours. If one line is busy, your call will automatically be routed to the next open line. The phone number is:

937-767-1468

2. Non-Business Hours: The Information Technology Center is unstaffed during non-business hours, however, voice mail is available to log your calls. A staff member will return your call as soon as possible. The following home phone numbers should be used only in an emergency situation:

937-681-6959 – Gary Bosserman, Director of Operations, MVECA

3. Facsimile Machine – 937-767-1793.

- **Downtime Schedule:**

There is no regularly scheduled downtime. If possible, a one-week notice will be given if downtime needs to be scheduled.



1. The upgrades of system software may require system down time on Saturday and Sunday. A one-week notice will be given to remind users of this particular downtime.
2. The computer will be unavailable about twice a year for system software upgrades. The upgrades take one or two days depending upon whether it is a major or minor upgrade. Two to three weeks notice will be given to users before this downtime occurs.

The MVECA Information Technology Center Staff is committed to providing you with the best possible service. If you have any problems or questions, please do not hesitate to call.

Regards,

Your MVECA Information Technology Staff:

Dean Reineke, Executive Director
Gary Bosserman, Director of Operations
Tom Faulkner, Treasurer/Financial Software Specialist
Thor Sage, Technology Coordinator
Jim Pesch, InfOhio Specialist
Tammy Hrosch, EMIS Software Specialist
Sandra Ingledue, SIS Software Specialist
Lynda Sidell, SIS Software Specialist
Annette Puckett, Software Specialist
Kelly Mader, Software Specialist
Deb Dinnen, Financial Software Specialist
Steve Phipps, Communications/Equipment Specialist
Sue Ann Welsh, Executive Secretary

Administrative Issues
System Issues
Financial Issues, Payroll, GAAP
Training, Technology Issues
InfOhio, MultiLis, Sirsi
EMIS, State Reporting
Student Services, DASL
Student Services, DASL
Student Services
Progress Book, Special Services
Payroll, GAAP, EMIS Financial
Hardware, troubleshooting, installation
Phones, invoices, registrations

ACCOUNT POLICIES AND PROCEDURES

I *Account Holder's Responsibilities*

- A. Account holders may use the computer system for business-related activities only. Users are expected to report all potential misuse to their appropriate supervisor and/or to the MVECA Director.
- B. Improper use includes, but is not limited to, the use of MVECA-owned and/or MVECA-operated computer systems and networks for the purpose of gaining unauthorized access to internal or external computer systems or accounts, for personal purposes, or for purposes of personal gain.
- C. Account holders are responsible to safeguard their passwords, other access protocols, school district and MVECA information, in whatever form.
- D. Printed output that is considered confidential shall not be printed on any common printer. Instead, it must be printed in a secure area or some other restricted area, such as the employee's office.



- E. Account holders will ensure that their account is protected from unauthorized access. Passwords are the computer's first line of defense against unauthorized system access. All users should adhere to the following password controls:
- Passwords shall be non-meaningful terms. Passwords should not be of a common nature such as last name, job title, children's names, street address, pet's names, etc.
 - Passwords should not be displayed, divulged, or accessible to or shared with others. If there is any reason to suppose that a password has become known, it should be changed immediately.
 - Passwords should never be written down, attached to the terminal, placed under the keyboard, or any other means that would allow for possible break-in.
 - Users should be aware of the LAST LOGIN time of his/her account and report to the MVECA Data Center Staff if it does not correspond with the last time they logged in.
 - Users should not put passwords into command files. The creation of user defined keys on the terminal with your password is also a breach in security.

II Account Management Policies

- A. Requests for new accounts must be submitted in writing using a MVECA Account Request Form. The approval process will include a written signature by the user and the user's immediate supervisor. This signature represents understanding and adherence to the policies contained in this document.
- B. Copies of the MVECA Account Request Form are available in both electronic and hardcopy formats. Either form can be obtained by contacting the MVECA Data Center.
- C. Account requests will be received Monday through Friday. The account request will be processed and available within five (5) business days of receipt of a properly filled out and signed form. The employee's immediate supervisor will receive a phone call confirming the account creation. The employee's supervisor should then notify the employee to contact the MVECA Data Center to receive his/her password. Passwords cannot be given to anyone other than the account holder.
- D. All user accounts will be created with default and authorized privileges of TMPMBX and NETMBX, except for those applications which require GROUP and/or GRPNAM. No additional privileges can be granted.
- E. All accounts will be set up with a two or three character district prefix and the users first initial and last name.
- F. The MVECA Data Center Staff will initially set passwords for new accounts. All initial passwords will be set up using the VMS password generator to ensure randomized passwords. It will be up to the employee to determine a proper password for subsequent changes. The initial password will be pre-expired; meaning it must be changed during the first login session.
- G. No GUEST accounts will be issued.



- H. For security reasons, each school district should immediately notify MVECA if an employee has been terminated or has left his/her organization. The accounts and files of terminated employees will be disabled immediately and the account and files will be deleted within five (5) business days.
- I. Similarly for security reasons, each school district should notify MVECA when any account holder is placed on a leave of absence, short-term or long-term disability. That person's account must be completely disabled. The account can be re-opened only at the request of the employee's immediate supervisor.
- J. Password controls for all accounts include the following:
- i All accounts are set to expire the password every 90 days. It is the user's responsibility to reset his/her own password. The password expiration will be 90 days from the time the password was last changed.
 - ii All Accounts will have a password minimum length of six (6) characters. Up to 31 characters may be used. Letters, numbers, dollar signs and the underscore character may be used in a password.
 - iii If a password is lost or forgotten, the user's supervisor must call the MVECA Data Center to establish a new one. The system stores passwords using a one-way encryption algorithm. After they are encrypted, passwords cannot be returned to their original readable form. Since there is no method to look up a user's password, a new pre-expired password will be generated.
 - iv Passwords may not be reused within a one-year period.
- K. Accounts that have no activity for 60 days will be disabled.



INSTRUCTIONS FOR COMPLETING THE ACCOUNT APPLICATION

Name Box – Print your first name, middle initial and last name.

Phone Box – Print your work phone number and extension – if applicable

Job Title Box – Print your job title, and the name you go by, if different than the name listed above.

School District Box – Print your school district name.

School Building Box – Print your school building name.

Supervisor's Name and Title Box – Print your immediate supervisor's name and title – if applicable.

Supervisor's Phone Number – Print supervisor's phone number and extension – if applicable.

Type of Request Box – Check whether this is a new account request, a request to delete an account, or a renewal of an existing account. For a renewal account, please indicate the Username of the existing account. If this is a renewal or deletion of an existing account, you can now skip directly to the REQUIRED SIGNATURES box.

Required Signatures Box – The person for whom the account is being created or renewed needs to sign and date the first line. The immediate supervisor of the applicant needs to sign and date the second line. The form cannot be processed without the correct signatures.

Statement of Need Box – Please check any and all that apply, including the read only boxes. If you need access to a restricted or queued printer, please indicate the printer name.

Note:

Please print all information except for signatures.

Only the two pages of the MVECA Authorized Account Application form needs to be returned. All other pages should be kept for future reference.



MIAMI VALLEY EDUCATIONAL COMPUTER ASSOCIATION
MVECA Authorized Account Application
 Revised 10/2007

First Name	Middle Initial	Last Name	Work Phone	Extension
Job Title		Called Name		
School District			School Building	
Supervisor's Name		Supervisor's Title	Supervisor's Phone and Ext.	
Type of Request				
<input type="checkbox"/> New Account		<input type="checkbox"/> Update		<input type="checkbox"/> Deletion
Current Username:				

Required Signatures

This form cannot be processed without the appropriate signatures.

Applicant:	x	Date:	
Immediate Supervisor:	x	Date:	

For access to Fiscal Area, EMIS Staff and Fiscal Data, Treasurer's signature is required:

Treasurer:	Date:
-------------------	--------------

For access to Staff Area and EMIS Area, Superintendent's signature is required:

Superintendent:	Date:
------------------------	--------------

Statement of Need (next page)

Please check all items you will need

Full Access allows the user to modify, display, delete and add

Read Only Access allows the user to read but will not allow modification in any way

Both full and read only access for the Fiscal Area requires the Treasurer's signature

Both full and read only access for Staff Area requires the Superintendent's signature



Statement of Need for:

Applicant:	
-------------------	--

FISCAL AREA		
<i>Full Access</i>		<i>Read Only</i>
<input type="checkbox"/>	USAS Accounting	<input type="checkbox"/>
<input type="checkbox"/>	EIS – Equipment Inventory	<input type="checkbox"/>
<input type="checkbox"/>	Inquiry Programs	<input type="checkbox"/>
<input type="checkbox"/>	Requisitions	<input type="checkbox"/>
<input type="checkbox"/>	Monthly CD	<input type="checkbox"/>

STAFF AREA		
<i>Full Access</i>		<i>Read Only</i>
<input type="checkbox"/>	USPS - Personnel	<input type="checkbox"/>
<input type="checkbox"/>	USPS Payroll	<input type="checkbox"/>
<input type="checkbox"/>	Payroll CD	<input type="checkbox"/>

FISCWEB Group: _____

EMIS AREA		
<i>Full Access</i>		<i>Read Only</i>
<input type="checkbox"/>	Student Data	<input type="checkbox"/>
<input type="checkbox"/>	Staff Data	<input type="checkbox"/>
<input type="checkbox"/>	Course Data	<input type="checkbox"/>
<input type="checkbox"/>	Fiscal Data	<input type="checkbox"/>
<input type="checkbox"/>	General Data	<input type="checkbox"/>
<input type="checkbox"/>	SSID Access	<input type="checkbox"/>