Finance Applications Security Management

Policies and Procedures Guide

Copyright Information

Related Documents

All

- Financial Application Support Signature Authorization
- Financial Application Support Designation of Security Management

Finance Manager

- Financial Application Support Designation of Security Management
- FAQ Security Authorization Changes
- Request for Security Modification – MAIN FORM
- Request for Security Modification – ACCOUNTING REPORTS & LOOKUP
- Request for Security Modification - AP CLERK
- Request for Security Modification - ATTENDANCE ENTRY
- Request for Security Modification - ATTENDANCE INQUIRY
- Request for Security Modification - BLANK
- Request for Security Modification - HR CLERK
- Request for Security Modification - PAYROLL CLERK
- Request for Security Modification - REQUISITION APPROVER
- Request for Security Modification - REQUISITION BO APPROVER
- Request for Security Modification - REQUISITION USER
- Request for Security Modification - TREASURER
- Request for Security Modification - BUSINESS OFFICIAL

nVision

- Request for Security ROLE Modification – nVision Financial Application
- Request for Security Modification – nVision Financial Application – CBO
- Request for Security Modification – nVision Financial Application
- Requisition Approval Path Setup Form – nVision Financial Application

Change History

Rev #	Date	Author	Section	Nature of Change
Draft	10/22/13	Tim Keller	All	Initial draft.
1	11/5/13	Tim Keller	Al	
1.01	04/10/14	Tim Keller	4.1	Update for System Manager Rights
2.0	04/01/16	Tim Keller	All	Added provisions for nVision
2.01	04/15/16	Tim Keller	3.5	Added nVision password policies

Conventions Used In This Document:

⚑	Important Box – Alerts the reader to essential information.

✉	Note Box – Alerts the user to supplementary information.

💣	Warning Box – Alerts the user to a vital step, process, potential data loss, or security threat.

❖   **Procedure Heading – is used to title a series of steps the reader is to follow**

1. First Step

2. Second step

    a. First sub step

    b. Second sub step

        i. First sub-sub step

Text Styles

Command Line – Text the reader would need to type into an application or command line

Computer text – Output examples a command line interface or window text
Example:
```
Microsoft Windows XP [Version 5.1.2600]
```

Bold – Indicates command text the user must enter or select, such as menu items, buttons, and commands.
Italics – indicate emphasis or user variables.
Angle brackets (>)– indicate the progression of menu choices the user should select in a graphical user interface (GUI)
Example:
File > **Print**.
Vertical bars (|) – Separate alternative, mutually exclusive arguments. Do not enter the bars themselves.
Example:
3.   NET USE {devicename | *} [password | *]

Square brackets ([ ] – Indicate optional elements. Do not enter the brackets themselves.
Example:
4.   DIR [drive:][path][filename]

Braces ({ }) – Indicate a required choice. Do not enter the braces themselves.
Example:
access-list *number* [{**permit** | **deny**}]

Double Angle brackets (< >)– Indicate arguments or operations in contexts that do not allow italics, and in examples indicate character strings a user enters that do not appear on the screen
Example:
<password>
Double quotes (" ")– Are used for Window titles.
Example:
"Windows Explorer"

1 Table of Contents

Purpose

This document is intended to provide EduTech staff with guidelines to manage finance application security and support.

In no way does this document supersede any established Wayne Finger Lakes BOCES, Genesee Valley Educational Partnership, or EduTech policies and procedures.

Audience

The primary audience for this document is EduTech staff persons who are tasked with supporting finance applications. Certain school district staff may also benefit from this document in order to gain a better understanding of the constraints in which EduTech application support functions.

Finance Application Support Policies and Procedures

1. **Security Authorization by Districts**
   1.1. Districts may designate EduTech as being responsible for managing system security for Finance Manager or nVision applications by submitting the Financial Application Support Designation of Security Management form to EduTech.
   1.2. If the district does not designate EduTech as the security administrator, they must indicate so by checking the appropriate box on the form.
   1.3. By authorizing EduTech to manage application security for finance applications, the district agrees to allow EduTech staff full access to the Finance Manager or nVision System Manager module, and read only access to all other modules. If the Requisitions module is installed, EduTech requires full access to that module to set up approval processes parameters.
   1.4. Additionally, EduTech application support requires access to the server on which Finance Manager or nVision is installed, the districts network, and end-user workstations

2. **Authorized Signatures**
   2.1. Each district which designates EduTech as the system and security administrator must also submit a signature authorization form stating who in the district is authorized to sign security change requests.
   2.2. Districts must have a minimum of one authorized signature for security changes.
   2.3. In addition to indicating the individuals authorized to sign for security changes, the district must designate the number of signatures required to make security requests.
   2.4. If any of the signatories leave the district or are replaced, a new signature authorization form must be submitted to EduTech with ALL authorized signatures.
   2.5. The most recently dated signature form supersedes any previously submitted form.

3.　User Account Management

　3.1.　New Users

　　3.1.1. EduTech requires a security form to be completed and signed for new user requests.

　　3.1.2. Districts may use the single page, main form, the more detailed role specific form, or the blank form for security requests depending on the amount of specific rights required.

　3.2.　Changes to Current User Accounts

　　3.2.1. Security change request for current users require a form to be completed indicating the appropriate rights changes. The form must be signed by an authorized district signatory and either faxed or e-mailed to EduTech.

　3.3.　Deletion of Users

　　3.3.1. A district may request that a user be removed or deleted from the system.

　　3.3.2. At the time of the request, all user rights will be removed, and the account disabled. This will allow the district to run audit reports on the individual account.

　　3.3.3. Once the district has completed their fiscal year-end audit, the account will be permanently deleted from the system.

　3.4.　Password Resets

　　3.4.1. Password reset requests can be handled by calling or e-mailing the EduTech Helpdesk at 1-800-722-5797, or finance@edutech.org.

　3.5.　Password Complexity

　　3.5.1. Finance Manager:

　　　3.5.1.1.　Due to limitations of the backend database, Progress, FM cannot force complex passwords for users.

　　3.5.2. nVision

- Passwords must meet the following complexity requirements:
- Not contain the user's account name or parts of the user's full name that exceeds two consecutive characters.
- Be at least Six characters in length
- Contain characters from three of the following categories
- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (e.g. !, $, #, %)
- Complexity requirements are enforced when passwords are changed or created

　　　3.5.2.1.　MS SQL 2014 Policy:

　　　　1.1.1..1. Enforce password history:　　24 passwords remembered

　　　　1.1.1..2. Maximum password age:　　60 days

　　　　1.1.1..3. Minimum password age:　　0 days

　　　　1.1.1..4. Minimum password length:　　8 characters

　　　　1.1.1..5. Passwords must meet complexity requirements:　　　　Enabled

　　　　1.1.1..6. Store passwords using reversible encryption:　　Disabled

3.6. Retention of Security Documents

   3.6.1. All security authorization, change, add, or delete forms are retained by EduTech for each district for a period of seven years.

4. **System Updates**

   4.1. Occasionally vendors will create new permissions or new functionality in the system requiring rights modifications. EduTech will notify each district of these changes along with the appropriate rights change request authorization form. If the district has designated EduTech as the security manager, we will add appropriate permissions to the support staff automatically. The district will not have to submit additional forms to grant these rights.

5. **Temporary Authorization for Read – Write Acces**s

   5.1. If EduTech staff is requested by the district to make changes to the data or enter data into the system, the district may submit the appropriate security change request form granting temporary rights. At the completion of the work, the district must submit a second form removing the rights of the EduTech user.

   5.2. No EduTech staff can make security changes to their own system account granting them write access to the software. Any rights requested by the district must be made by EduTech staff other than the person being requested by the district. The EduTech staff, being given access to the system will have their System Manager access temporarily disabled for the duration of the request.

6. **Conflicts of Interest**

   6.1. Board of Education Membership

      6.1.1. EduTech employees are regularly involved in various activities within their home school districts. If in the case an EduTech employee sits on the school board of a component school district, the EduTech employee will not be involved with any day to day operational activities of the school district. Support provided to the district by the employee in question will be limited.

   6.2. User Rights

      6.2.1. Once EduTech is notified that the employee serves on the board of their home school district, the system manager and all other user rights will be disabled for that employee.

   6.3. Day to Day Support Activities

      6.3.1. The employee will be discouraged from providing regular support to the district and will defer any support requests to other team members if possible.

   6.4. Special Exceptions

      6.4.1. If a scenario occurs that it is necessary for the EduTech employee to be involved in a support activity for the school district. The district superintendent will be notified by the EduTech manager supervising that employee. The employee will only provide support if both the superintendent and the EduTech manager are in consensus of the parameters of the activity.

7. **Remote Desktop Support**

   7.1. EduTech Application Support utilizes a remote desktop support tool called Bomgar. Remote sessions are initiated by the end-user and cannot be initiated by EduTech Application support. The end-user must authorize a remote session before it begins, otherwise it will not initiate.

   7.2. Bomgar requires the installation of a small executable file to be installed onto a client workstation which is deleted at the end of the session. In cases where districts do not allow end-users to install software, or have the temporary files locations locked down in the operating system, we can work with the district IT staff to allow remote sessions via Bomgar to function.

8. **Remote Backup of Data**

   8.1. EduTech Application Support creates a nightly back-up of district application data in order to ensure our ability to provide adequate support to our districts. These backups are for purposes of troubleshooting errors, and creating data extracts. In some cases this data may be used to recover from an application or hardware failure, but should not be considered part of the district's disaster recovery plan.

   8.2. We maintain 1 week of nightly backups, one weekly backup, and one monthly backup for one year.

9. **Confidentiality of Data**

   9.1. In order to provide support to our districts the EduTech Application Support team often requires access to privileged district data. This privileged access imposes a high level of responsibility and an obligation to ensure that the access to the data is done in an ethical, professional and legal manner.

   9.2. EduTech Application Support will take every precaution to prevent unnecessary or unauthorized access to district data.

   9.3. EduTech will limit access to district data to authorized staff.

   9.4. The Application support team will treat the data as confidential.

   9.5. All data will not be shared, duplicated, altered, or deleted without notice to and authorization from the district.

2 Administrative Applications Support Employee Acknowledgement

By signing below,

1. I confirm that I have received the Finance Application Security policies and procedures.

2. I also attest that I have read them completely and thoroughly, understand them to the fullest extent.

3. I agree to abide by the guidelines they establish.

4. If at any time I am unclear about a policy or have a question I will consult my Manager for further guidance.

_____   _____

(Employee Name – Printed)   (Date)

_____

(Employee Signature)

Please Return This Page To Your Manager.