TO: **ALL COUNTY PERSONNEL**

FROM: **VERDENIA C. BAKER**
COUNTY ADMINISTRATOR

PREPARED BY: **OFFICE OF FINANCIAL MANAGEMENT & BUDGET (OFMB)**

SUBJECT: **COMPUTER SECURITY FOR THE COUNTY'S AUTOMATED FINANCIAL SYSTEM**

PPM #: **CW-F-020**

==========

ISSUE DATE	**EFFECTIVE DATE**
June 6, 2022	June 6, 2022

==========

PURPOSE:

To provide County departments and other users of the County's automated financial system with security guidelines in order to maintain system integrity.

UPDATES:

Future updates to this PPM are the responsibility of the Director of OFMB.

SCOPE:

This PPM covers the County's centralized accounting and financial system and all subsystems.

AUTHORITY:

- Palm Beach County Administrative Code, Section 403.00, as may be amended.

POLICY:

I. Passwords and User Identifications (User ID)
All transactions in the County's automated financial system will be electronically authorized by using passwords User ID. The use of passwords and User IDs will ensure that only authorized individuals can initiate or approve transactions or table entries and updates in the system. The password is known only to the individual and it is essential that the person using the password and assigned User ID is actually the person authorized to complete the transaction. In many cases, this electronic authorization replaces a physical signature.

The "System Administrator" of the Clerk's Office will create all financial system User accounts with the same User ID as that established for the user in the County's Universal Security Identity Management (SIM) system. Authentication of all Advantage Financial system users is done through SIM via lightweight directory access protocol each time a user provides the correct User ID and password at login.

The password must not be revealed under any circumstances. Should the individual forget his/her password, or if it becomes compromised in some way, they must reset their password online under the Universal Password System on the PBC intranet website or contact the ISS help desk for assistance in the issuance of a new password.

Each user will be required to sign a disclosure acknowledging responsibility for the User ID that they will be assigned. **Unauthorized and inappropriate use of any password or User ID by a County employee will be cause for disciplinary action, up to and including dismissal.**

II. User Security Roles, Workflow Roles and Override Authority (User Access)

User Access is initially determined by the Department Head or Fiscal Director. **It is suggested, for best practice and strongest internal controls, the same person who creates/initiates transactions should not have the authority to approve the transactions.**

III. User Restrictions

There are no restrictions on inquiries in the financial system except for certain security and other sensitive information such as but not limited to: W-9 attachments, Taxpayer Identification Numbers (TIN's) and bank account numbers.

IV. Changes in User Responsibilities

It is the department's responsibility to keep the System Administrator informed about personnel changes. User IDs must be deactivated when an employee is terminated. When an employee transfers, approval authority in the old department must be deactivated. Also, as job responsibilities change, User's roles must be modified to reflect the changed responsibility.

Communicating personnel changes or requests for changes to a User ID's role assignments should be in writing and signed by the Department Head or Fiscal Director using the applicable Security Request Form. Memos with the appropriate information, in lieu of a Security Request Form, will be acceptable during the semi-annual review process. If the System Administrator in the Clerk's Office is made aware (via report, e-mail or other form of communication) that an employee has separated from their home department (as indicated on the current security request form), the Administrator will deactivate the user and remove all user access in Advantage.

PROCEDURES:

Adding, Changing or Deleting System Users

For user access to be added or changed, an Advantage Security Request form (SRF) must be completed and signed by the Department Head or Fiscal Director and submitted to the System Administrator in the Clerk's Office. Additionally, new users are required to sign, date and submit the Computer Security Disclosure Form (Attachment A) to the System Administrator before the User ID will be created. For name changes and deactivations, a SRF is recommended but not required.

VERDENIA C. BAKER
COUNTY ADMINISTRATOR

Supersession History:
1. PPM # CW-F-020, issued 2/1/91
2. PPM# CW-F-020, effective 12/1/97
3. PPM# CW-F-020, effective 8/1/05
4. PPM# CW-F-020, effective 11/23/11
5. PPM# CW-F-020, effective 1/13/17

Attachment A

Interoffice Communication

FROM: **Verdenia C. Baker**
County Administrator

SUBJECT: COMPUTER SECURITY DISCLOSURE FORM

The System Administrator of the Clerk's Finance Department will be granting you access to the Advantage financial system. Your login to the financial system will be the same as your PBC SIM account User ID and Password. This User ID, and the password you choose, are yours alone and no other person has access to them.

All transactions entered with this User ID are credited to you. You are fully responsible for any transaction entered with this User ID. In the event that you forget your password, you may reset your password online under the Universal Password System on the PBC intranet website.

This User ID represents a significant responsibility. There should never be a need to reveal your password to anyone, not even your supervisor. If someone should ask for your password, direct them to your supervisor or the System Administrator. YOU MUST NOT REVEAL PASSWORDS OR OTHER CODES TO ANYONE. COMPROMISING THIS RESPONSIBILITY IS GROUNDS FOR DISCIPLINARY ACTION, UP TO AND INCLUDING DISMISSAL.

Your User ID will be given access to those functions deemed necessary for your job. Should the need arise for further access for which you do not have expressed authority, contact your supervisor to submit a new security form to the System Administrator. UNAUTHORIZED ACCESS IS GROUNDS FOR DISCIPLINARY ACTION, UP TO AND INCLUDING DISMISSAL.

Please print your name below, sign and date this form, and return to the System Administrator of the Clerk's Finance Department.

I understand my responsibilities with respect to any User ID assigned to me. I will not reveal my password, nor will I seek to perform transactions outside the scope of my responsibility. I will immediately report any suspicious transactions or any compromises of my password's security to my supervisor or the System Administrator. If I have knowledge that another person's password has been compromised, I will inform my supervisor or the System Administrator.

Name (Print) _____

Signature_____ Date_____