ADDENDUM TO GOVERN USE OF SOCIAL SECURITY NUMBERS FOR HUMAN RESOURCES/PAYROLL SYSTEMS

This addendum shall govern the District's use of social security numbers ("SSNs") in their human resources/payroll systems reporting databases.

In light of the consideration provided for in the LICENSE CONTRACT FOR USE OF SOFTWARE PERSONAL COMPUTER PRODUCTS FOR DISTRICT USE OF HRS AND/OR PSFS DATA the District agrees to indemnify and hold harmless LACOE from and against any and all demands, debts, liens, claims, losses, damages, liability, costs, expenses (including, but not by way of limitation, attorney's fees and costs actually incurred, whether or not litigation has commenced), judgments or obligations, actions, or causes of action whatsoever, for or in connection with injury, damage, or loss (including, but not limited to death) to any person or property related to the District's use of social security numbers in its human resources/payroll systems reporting databases including, but not limited to the following:

- Allegations concerning the theft, loss or unauthorized disclosure of personally identifiable non-public information that is in the care, custody, or control of the District.
- Acts or incidents that directly result from the failure of computer security to prevent a security breach including:
    - Alteration, corruption, destruction, deletion, distribution or damage to a data asset stored on computer systems;
    - Failure to prevent transmission of malicious code from computer systems to third party computer systems;
    - Participation in a denial of service attack directed against a third party computer system.
- Failure to timely disclose any of the above in violation of any breach notice law.
- Failure to comply with a privacy policy involving the disclosure, sharing or selling of personally identifiable non-public information.
- The failure to administer an identity theft prevention program.

In the District's use of social security numbers in its human resources/payroll systems reporting databases, the District agrees to the following practices and procedures:

- The District will not publicly display social security numbers.
- The District will not send documents with social security numbers on them through the mail, except on applications or forms or when required by law.
- When sending applications, forms or other documents required by law to carry SSNs through the mail, the District will place the SSN where it will not be revealed by an envelope window. Where possible, leave the SSN field on forms and applications blank and ask the individual to fill it in before returning the form or application.
- The District will not send SSNs by in any electronic form unless the connection is secure or the SSN is encrypted.
- The District will not require an individual to send his or her SSN over the internet or email, unless the connection is secure or the SSN is encrypted.

- The District will not require individuals to use SSNs as log on IDs, passwords or codes for access to Internet web sites or other services.
- The District will limit access to records containing SSNs only to those who need to see the numbers for performance of their duties. The District will protect records containing SSNs, including back-ups, during storage by encrypting the numbers in electronic records or storing records in other media in locked cabinets.
- The District will not store records containing SSNs on computers or other electronic devices that are not secured against unauthorized access.
- If SSNs are disclosed inappropriate and the individuals whose SSNs were disclosed are put at risk of identity theft or other harm, promptly notify the individuals potentially affected.
- The District will require employees to promptly report any inappropriate disclosure or loss of records containing SSNs to their supervisors.
- The District shall comply with Labor Code section 226(a) which requires employers to print no more than the last four digits of an employee's SSN or to use an employee ID number other than an SSN, on employee pay stubs or itemized statements.

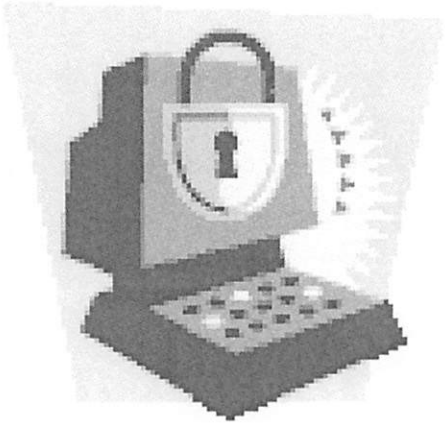
In the event that LACOE is served with, or otherwise becomes aware of a claim that pursuant to the terms of this agreement, the District shall be responsible for the defense of LACOE against the allegations made in such claim. LACOE shall provide the District reasonably timely written notice of same, and thereafter the District shall at its own expense defend, protect and save harmless LACOE against said claim or any loss or liability thereunder.

In the further event that the District fails to so defend and/or indemnify and save harmless, then LACOE shall have full rights to defend, pay or settle said claim on its behalf without further notice to the District and with full rights to recourse against the District for all fees, costs, expenses and payments made or agreed to be paid to discharge said claim.

LOS ANGELES COUNTY OFFICE OF EDUCATION	WILLIAM S. HART UNION HIGH SCHOOL DISTRICT
By_____	By_____
Patricia Smith Interim – Chief Financial Officer Business Services	_____ Typed or Printed Name
	_____ Title
Date_____	Date _____
	Indicate Federal I.D. Number:
	_____

PC Products Labels, Lists & Letters and Labor

System Security Modification



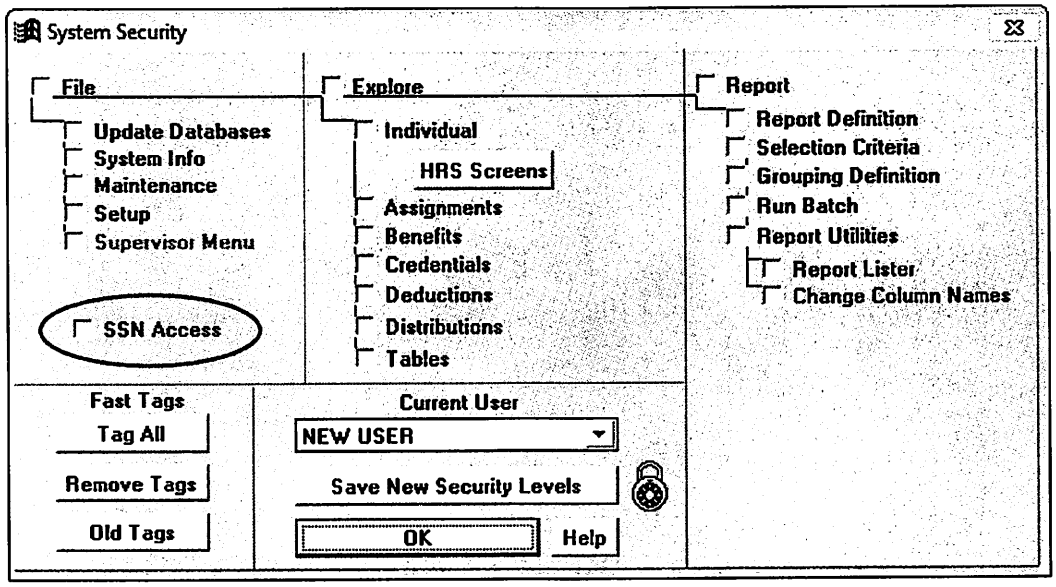
LACOE Division of School Financial Services
PC Budget, PC Products & District Support Unit

PC Products Labels, Lists, & Letters (LLL) and Labor
System Security Modification

Description **Page**

PC LLL and PC Labor System Security Modification

The **SSN Access** field has been added to the **System Security** screen in PC LLL and PC Labor. This feature allows each district's system security supervisor to limit user access to the 9-digit SSN. It is very important for districts that elect to include the 9-digit in their PC LLL and PC Labor data files to utilize this feature. Districts that do not elect to include the 9-digit SSN in their data files can also utilize this feature but it is not as important to do so because only the last four (4) digits of the SSN preceded by X's in the first five positions of the SSN are included in their data files, e.g., XXX-XX-0533.



We strongly recommend each district carefully review PC LLL and PC Labor users' job responsibilities and only make the 9-digit SSN fields (Employee SSN, Prior SSN and Dependent SSN) available to employees who actually need access to the complete SSN to perform their job duties. We also recommend:

1. Limiting **Supervisor Menu** access to a few key staff. Users with access to the **Supervisor Menu** can provide SSN access to themselves or other users at any time.
2. Assigning each user a unique user ID and password if users currently use the same user ID and password.
3. Assigning users with SSN access new passwords in the event passwords were previously shared with others.
4. Stressing the importance of users logging out of the application when away from workstations.

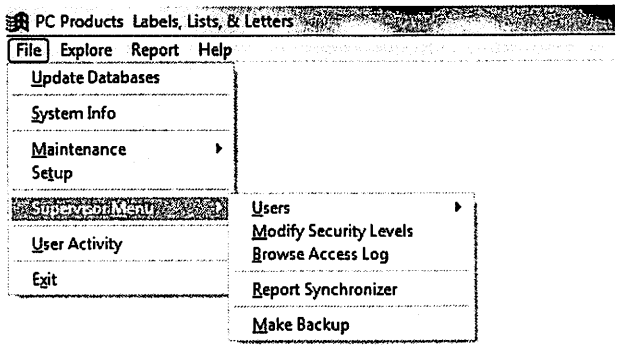
Examples for modifying common user security access levels for PC LLL and PC Labor are provided in the next sections of this document. The process for updating user security for both applications is similar.

PC LLL User with Supervisor Menu Access

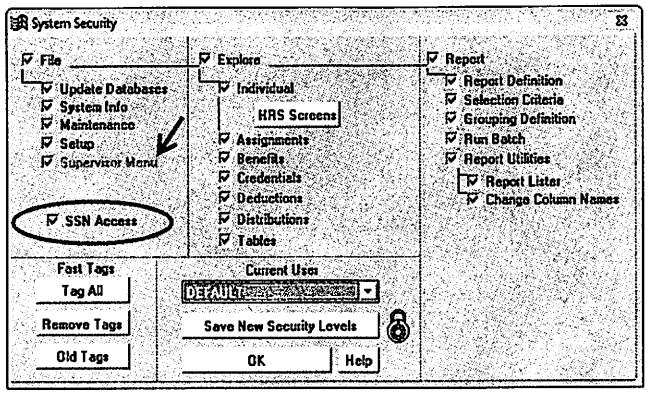
PC LLL users with access to the **Supervisor Menu** have the ability to access all application data and functionality. Only district staff responsible for system security administration should have access to the **Supervisor Menu**.

To Modify Security Levels of User with Supervisor Menu Access:

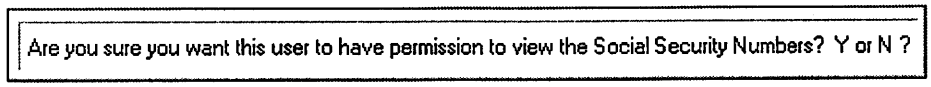
1. Go to **File | Supervisor Menu | Modify Security Levels.**



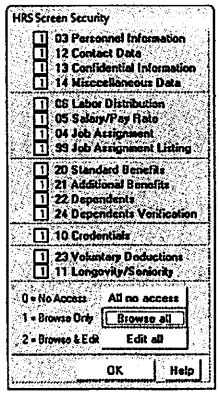
2. When the **Supervisor Menu** checkbox contains a check mark, the user has access to the **Supervisor Menu**. If the user is to no longer have access, uncheck the box in front of **Supervisor Menu.**
3. To provide access to the 9-digit SSN, check the box in front of **SSN Access.**



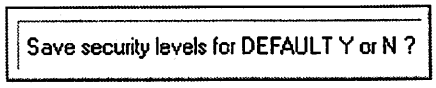
4. After checking the box in front of **SSN Access,** the following prompt will appear in the upper right corner of the screen to confirm that system security supervisor wants user to have access to the 9-digit SSN. Enter "**Y**" if user is to have access to the 9-digit SSN or "**N**" if user is not to have access to the 9-digit SSN. If "N" is entered, the application will remove the check mark from the **SSN Access** checkbox.



5. Click **HRS Screens** to access **HRS Screen Security**. For this example, **"1" Browse Only** is selected for all screens. If user is not to have access to one or more HRS screens, enter **"0" No Access** as appropriate.



6. Click **OK** after **HRS Screen Security** is completed. System security supervisor is returned to **System Security** screen.
7. Click **Save New Security Levels**. The following prompt will appear in the upper right corner of the screen to verify that system security supervisor wants to save change(s) to user's security. Enter **"Y"** to save change(s) or **"N"** to discard change(s).

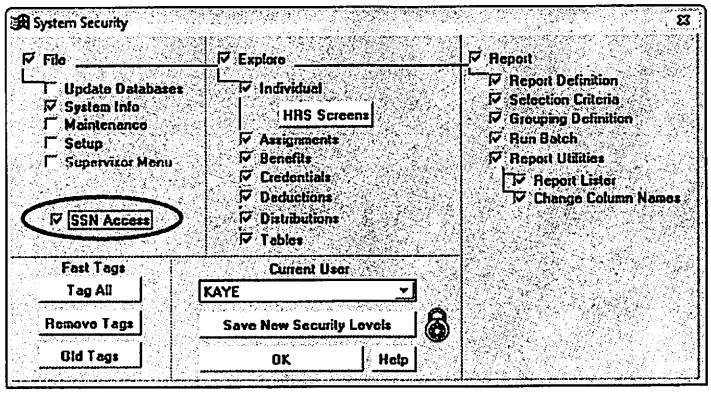


PC LLL User with SSN and HRS Screens Access

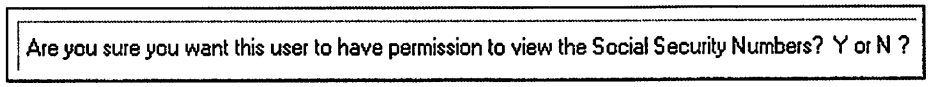
PC LLL user has access to 9-digit SSN, access to all HRS screens, explore and report functionality, which includes the ability to generate Excel, database and other types of output files.

To Modify Security Levels of User to Include SSN Access:

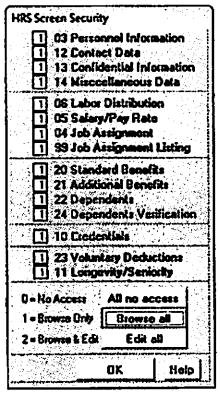
1. Go to **File | Supervisor Menu | Modify Security Levels.**
2. To provide access to the 9-digit SSN, check the box in front of **SSN Access.**



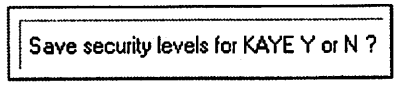
3. After checking the box in front of **SSN Access**, the following prompt will appear in the upper right corner of the screen to confirm that system security supervisor wants user to have access to the SSN. Enter "**Y**" if user is to have access to the SSN or "**N**" if user is not to have access to the SSN. If "N" is entered, the application will remove the check mark from the **SSN Access** checkbox.



4. Click **HRS Screens** to access **HRS Screen Security**. For this example, **"1" Browse Only** is selected for all screens. If user is not to have access to one or more HRS screens, enter **"0" No Access** as appropriate.



5. Click **OK** after **HRS Screen Security** is completed. System security supervisor is returned to **System Security** screen.
6. Click **Save New Security Levels**. The following prompt will appear in the upper right corner of the screen to verify that system security supervisor wants to save change(s) to user's security. Enter "**Y**" to save change(s) or "N" to discard change(s).



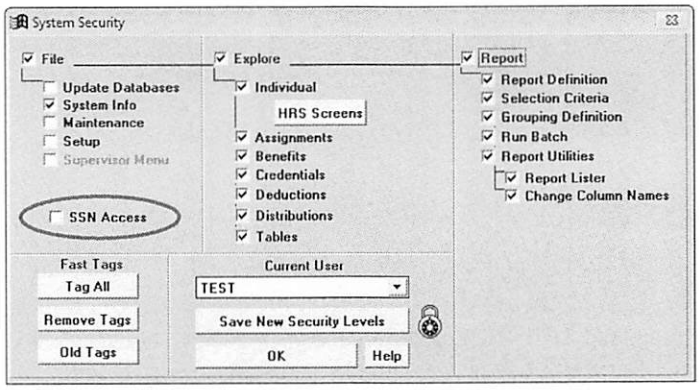
PC LLL User without SSN Access

PC LLL user does not have access to 9-digit SSN or HRS Screens **22** and **24**. User has access to explore and report functionality, which includes the ability to generate Excel, database and other types of output files. User is not able to view, print or export the 9-digit SSN.

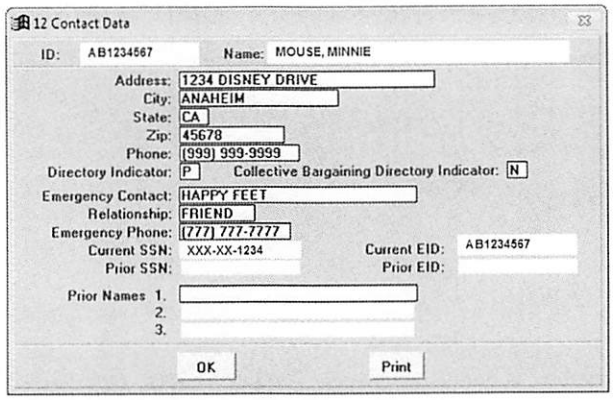
To Modify Security Levels of User to Exclude SSN Access:

1. Go to **File | Supervisor Menu | Modify Security Levels.**

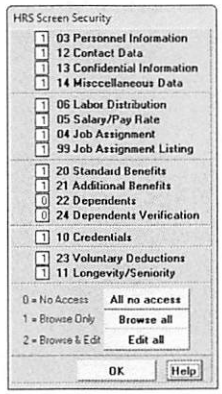
2. Do not check the box in front of **SSN Access**. If the box is already checked, remove the check mark.



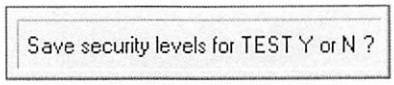
3. When user does not have SSN access, the first five (5) digits of SSN will populate with X's followed by the last four (4) digits of the SSN, e.g., XXX-XX-1234. This partial SSN will be displayed on screens, on formatted reports and in export files. See sample screen shot below.



4. Click **HRS Screens** to access **HRS Screen Security**. For this example, **"1" Browse Only** is selected for all screens, except **22** and **24**. For HRS screens **22** and **24**, "**0**" is entered to prevent user from accessing these screens.



5. Click **OK** after **HRS Screen Security** is completed. System security supervisor is returned to **System Security** screen.
6. Click **Save New Security Levels**. The following system prompt will appear in the upper right corner of the screen to verify that system security supervisor wants to save change(s) to user's security. Enter "**Y**" to save change(s) or "N" to discard change(s).

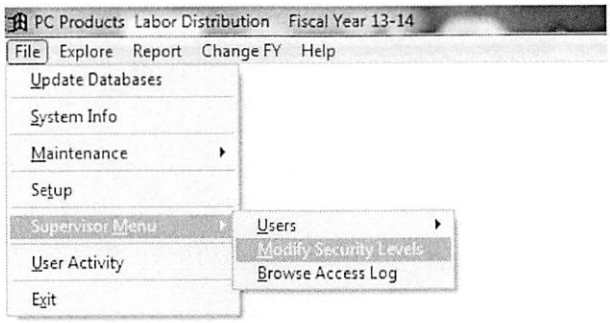


PC Labor User with Supervisor Menu Access

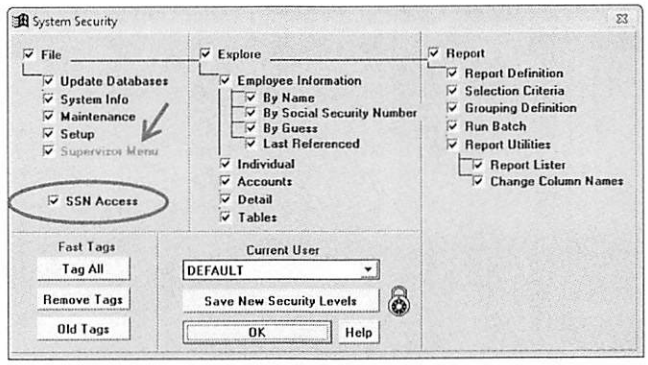
PC Labor users with access to the **Supervisor Menu** have the ability to access all system data and functionality. Only district staff responsible for system security administration should have access to the **Supervisor Menu**.

To Modify Security Levels of User with Supervisor Menu Access:

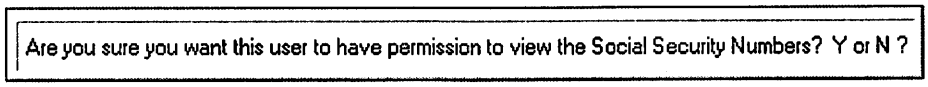
1. Go to **File | Supervisor Menu | Modify Security Levels**.



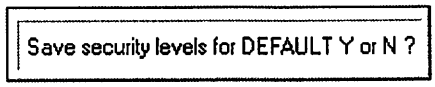
2. When the **Supervisor Menu** checkbox contains a check mark, user has access to the **Supervisor Menu**. If user is to no longer have access, uncheck the box in front of **Supervisor Menu**.
3. To provide access to the 9-digit SSN, check the box in front of **SSN Access**.



4. After checking the box in front of **SSN Access**, the following prompt will appear in the upper right corner of the screen to confirm that system security supervisor wants user to have access to the SSN. Enter "**Y**" if user is to have access to the SSN or "**N**" if user is not to have access to the SSN. If "**N**" is entered, the application will remove the check mark from the SSN Access checkbox.



5. Click **Save New Security Levels**. The following prompt will appear in the upper right corner of the screen to verify that system security supervisor wants to save change(s) to user's security. Enter "**Y**" to save change(s) or "**N**" to discard change(s).

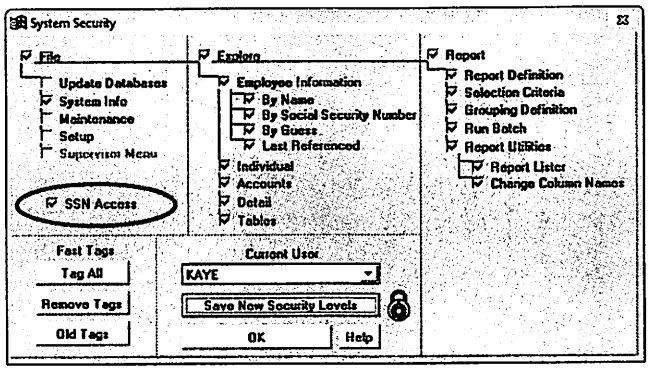


PC Labor User with SSN Access

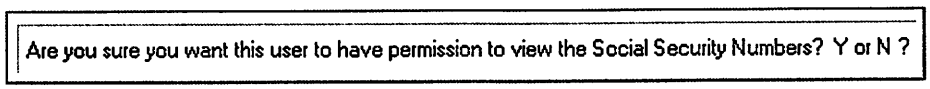
PC Labor user has access to 9-digit SSN, explore and report functionality, which includes the ability to generate Excel, database and other types of output files.

To Modify Security Levels of User to Include SSN Access:

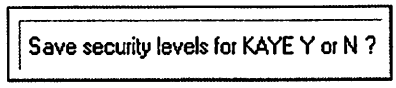
1. Go to **File I Supervisor Menu I Modify Security Levels.**
2. To provide access to the 9-digit SSN, check the box in front of **SSN Access.**



3. After checking the box in front of **SSN Access**, the following prompt will appear in the upper right corner of the screen to confirm that system security supervisor wants user to have access to the SSN. Enter "**Y**" if user is to have access to the SSN or "**N**" if user is not to have access to the SSN. If "N" is entered, the application will remove the check mark from the **SSN Access** checkbox.



4. Click **Save New Security Levels**. The following prompt will appear in the upper right corner of the screen to verify that system security supervisor wants to save change(s) to user's security. Enter "**Y**" to save change(s) or "**N**" to discard change(s).

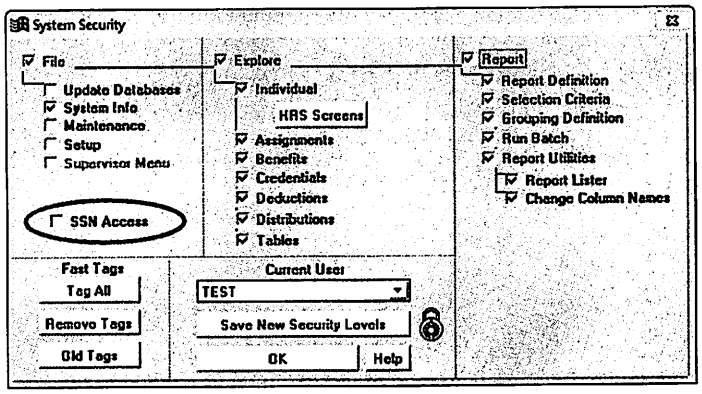


PC Labor User without SSN Access

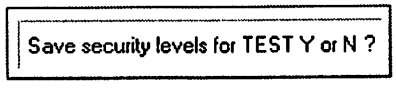
PC Labor user does not have access to 9-digit SSN. User has access to explore and report functionality, which includes the ability to generate Excel, database and other types of output files. User is not able to view, print or export the 9-digit SSN.

To Modify Security Levels of User to Exclude SSN Access:

1. Go to **File I Supervisor Menu I Modify Security Levels.**
2. Do not check the box in front of **SSN Access**. If the box is already checked, remove the check mark. When user does not have SSN access, the first five (5) digits of SSN will populate with X's followed by the last four (4) digits of the SSN, e.g. XXX-XX-1234. This partial SSN will be displayed on screens, on formatted reports and in export files.



3. Click **Save New Security Levels**. The following system prompt will appear in the upper right corner of the screen to verify that system security supervisor wants to save change(s) to user's security. Enter "**Y**" to save change(s) or "**N**" to discard change(s).



PC Products Support

Please contact the PC Budget, PC Products and District Support Unit at (562) 922-8683 if you have questions regarding the new PC Product security feature or need assistance. You may also contact Richard Skaar at (626) 465-8957 or Meus Binsol at (626) 864-0336.