How to…

And Why
Implement
Security in
Time Matters

Prepared October 10, 2011 by:

Kathy Burger Consulting, LLC

732-279-6301 ***Office***
609-238-2967 ***Cell***

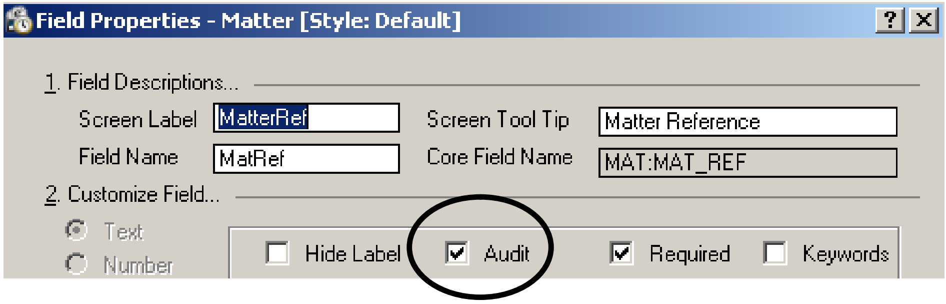
Kathy@kathyburgerconsulting.com

Many law firms do not think about security in Time Matters. Their office staff members are loyal, often family, and completely trustworthy. These firms do not see security as an issue.

Some security settings, however, have nothing to do with trust or breaches of confidentiality. This paper provides some examples.

Audit:

One of the simplest ways to protect your data is to use the "Audit" feature in Time Matters. Right click in a field and select customize field. On the resultant box, check to Audit.


Field Properties - Matter [Style: Default]

1. Field Descriptions...

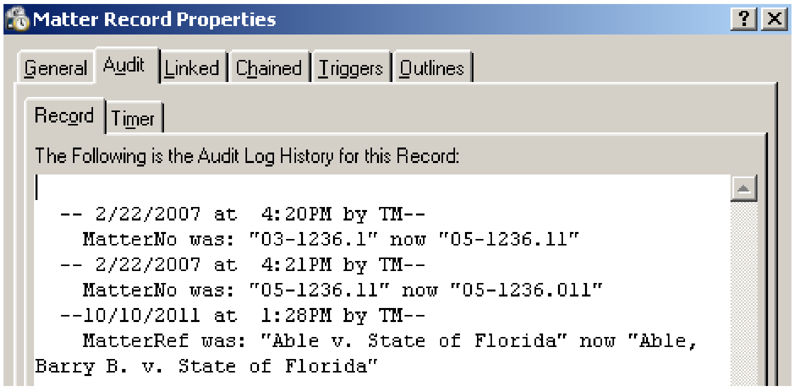
Screen Label: MatterRef
Screen Tool Tip: Matter Reference
Field Name: MatRef
Core Field Name: MAT:MAT_REF

2. Customize Field...

● Text
○ Number

□ Hide Label ☑ Audit ☑ Required □ Keywords

When data in the field is changed, information on the prior contents, the date of the change, and the user who made the change lists on the audit tab of the properties of the record.



The Following is the Audit Log History for this Record:

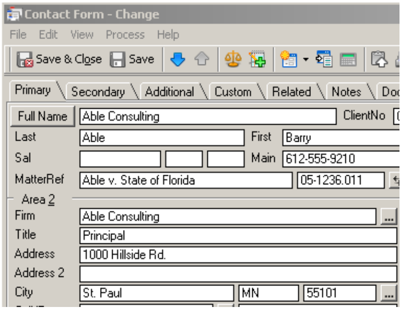
```
  -- 2/22/2007 at  4:20PM by TM--
    MatterNo was: "03-1236.1" now "05-1236.11"
  -- 2/22/2007 at  4:21PM by TM--
    MatterNo was: "05-1236.11" now "05-1236.011"
  --10/10/2011 at  1:28PM by TM--
    MatterRef was: "Able v. State of Florida" now "Able,
Barry B. v. State of Florida"
```

Client Contact Information:

A change of client information is most effective when applied to the contact record. In this way, the changes made propagate to related records automatically.

Let's say Susie the secretary calls Barry Able to confirm an upcoming appointment. Barry advises Susie he has moved his office. If Susie updates Barry's address in the Event Record, the contact, the matter(s), and other related records will retain the

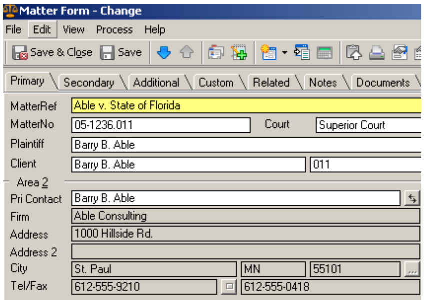
old address. Avoid this by protecting the address fields on related records from changes. Susie will be forced to go to the Contact record to enter the new data.
In the screenshots below, changes to address and phone number fields cannot be affected from a Matter or an Event because you cannot click into them. Those fields have been protected from changes through field-level security settings.


Contact Form - Change
File Edit View Process Help
Save & Close Save
Primary Secondary Additional Custom Related Notes Doc

Full Name	Able Consulting	ClientNo	
Last	Able	First	Barry
Sal		Main	612-555-9210
MatterRef	Able v. State of Florida	05-1236.011	

Area 2

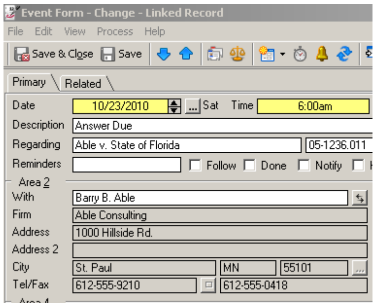
Firm	Able Consulting		
Title	Principal		
Address	1000 Hillside Rd.		
Address 2			
City	St. Paul	MN	55101


Matter Form - Change
File Edit View Process Help
Save & Close Save
Primary Secondary Additional Custom Related Notes Documents

MatterRef	Able v. State of Florida		
MatterNo	05-1236.011	Court	Superior Court
Plaintiff	Barry B. Able		
Client	Barry B. Able	011	

Area 2

Pri Contact	Barry B. Able		
Firm	Able Consulting		
Address	1000 Hillside Rd.		
Address 2			
City	St. Paul	MN	55101
Tel/Fax	612-555-9210	612-555-0418	


Event Form - Change - Linked Record
File Edit View Process Help
Save & Close Save
Primary Related

Date	10/23/2010	Sat	Time 6:00am
Description	Answer Due		
Regarding	Able v. State of Florida	05-1236.011	
Reminders		□ Follow □ Done □ Notify □	

Area 2

With	Barry B. Able		
Firm	Able Consulting		
Address	1000 Hillside Rd.		
Address 2			
City	St. Paul	MN	55101
Tel/Fax	612-555-9210	612-555-0418	

To get to the contact record from a related record, right-click the field with the contact lookup, and select “Open Contact Record”. There is a caveat; the automatic relationship must be set. Check the lookup button to the right of the field. You want arrows and not dots.

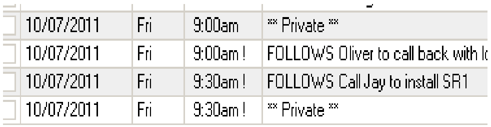
Like this ⇆. Not like this .... Get this effect by selecting the contact from the popup list that opens when you click the lookup button or hit the F2 key.

Private Event Records:

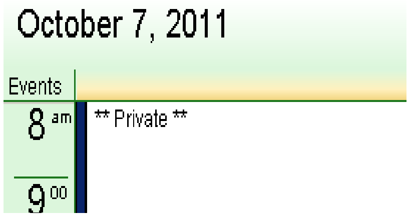
Staff may want personal appointments to show in the calendar without revealing any personal information.

A simple setting in the user dialogue box, on the access tab, allows for hiding or showing as private any records belonging to other staff where the private box is check marked. (Screenshot can be seen at the bottom of page 4.)

On the Calendar, and in the Event List, the record can be made to list with the description ** Private **. In that way conflicting calendar entries are avoided, but the contents of the record are not revealed and the record cannot be opened.



10/07/2011	Fri	9:00am	** Private **
10/07/2011	Fri	9:00am !	FOLLOWS Oliver to call back with I
10/07/2011	Fri	9:30am !	FOLLOWS Call Jay to install SR1
10/07/2011	Fri	9:30am !	** Private **

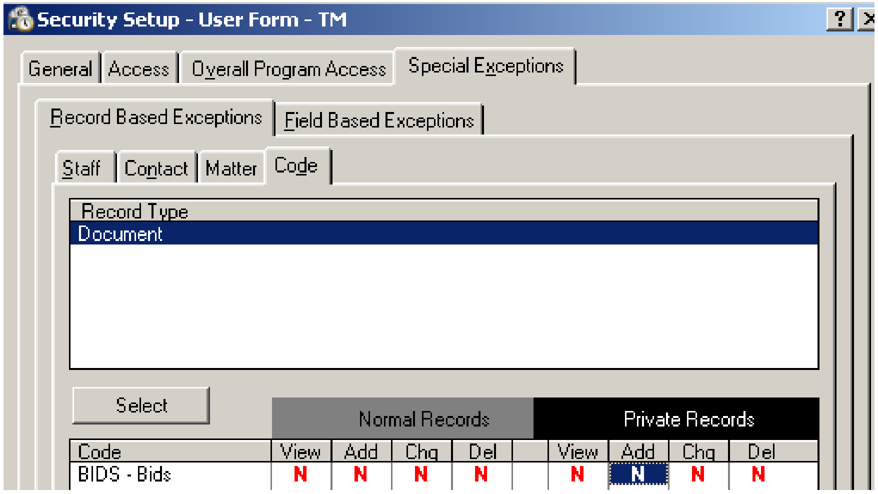


** Private **

Private Document Records:

The firm may have document records that are confidential and should only be available to particular staff. Examples are employment records, tax records, and financial reports. A good way to reduce exposure of these types of records is to use security settings by code.

Any document record with the classification code 'BIDS' will not be seen by the staff whose settings are shown below*.



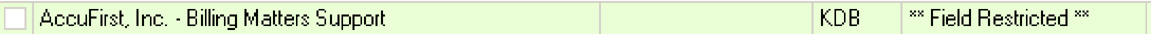
Record Type
Document

	Normal Records				Private Records			
Code	View	Add	Chg	Del	View	Add	Chg	Del
BIDS - Bids	N	N	N	N	N	N	N	N

*Keep in mind that the documents themselves CAN be accessed if the user browses to them through windows explorer. Additional security can be put in place to direct the documents to a shared location that is not accessible to all staff through workstation settings, network mapping, and windows profiles. Your IT person can help set it up.

Protect Confidential Content:

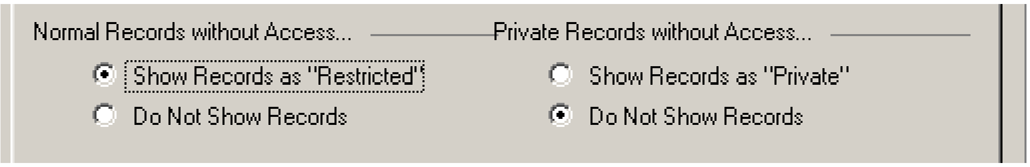
Not only can information entered on a matter or other form be protected from changes, it can be also be hidden from view. In the example below, data entered into a matter field appears to staff as restricted both on the form and in the list.



□	AccuFirst, Inc. - Billing Matters Support		KDB	** Field Restricted **

The field can be set to be hidden, and not show at all, or show as it does above, with the words **Field Restricted**.

The setting is on the Access tab of the User Settings.

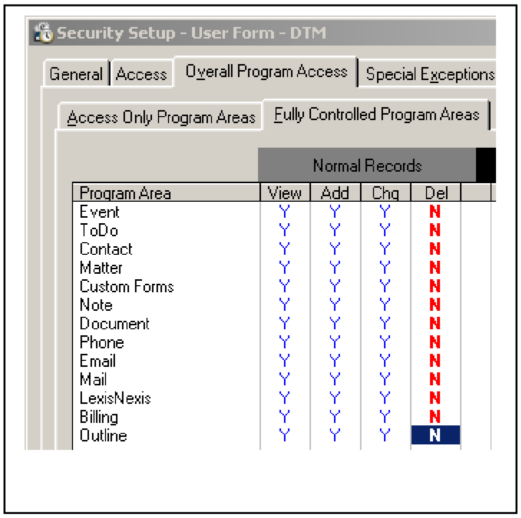


Normal Records without Access...
● Show Records as "Restricted"
○ Do Not Show Records

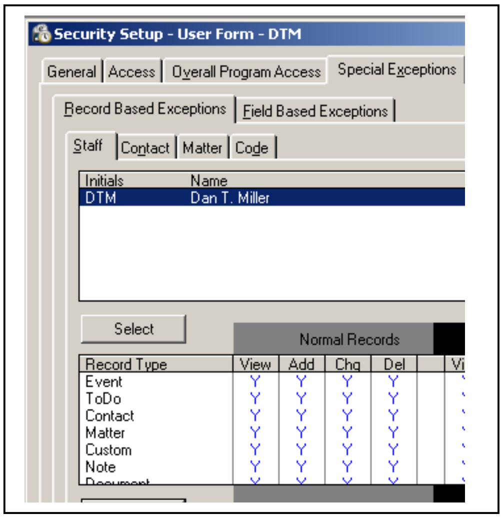
Private Records without Access...
○ Show Records as "Private"
● Do Not Show Records

Delete Records:

To avoid the accidental deletion of records, limit who, if anyone can delete Contacts, Matters, Bill Items, Events, etc. With the settings shown below, a user cannot delete certain record types. However, a Special Exception can be set so that the user CAN delete records with his default staff in the staff field.


Security Setup - User Form - DTM
General
Access
Overall Program Access
Special Exceptions
Access Only Program Areas
Fully Controlled Program Areas
Normal Records

Program Area	View	Add	Chg	Del
Event	Y	Y	Y	N
ToDo	Y	Y	Y	N
Contact	Y	Y	Y	N
Matter	Y	Y	Y	N
Custom Forms	Y	Y	Y	N
Note	Y	Y	Y	N
Document	Y	Y	Y	N
Phone	Y	Y	Y	N
Email	Y	Y	Y	N
Mail	Y	Y	Y	N
LexisNexis	Y	Y	Y	N
Billing	Y	Y	Y	N
Outline	Y	Y	Y	N



Initials	Name
DTM	Dan T. Miller

Record Type	View	Add	Chg	Del
Event	Y	Y	Y	Y
ToDo	Y	Y	Y	Y
Contact	Y	Y	Y	Y
Matter	Y	Y	Y	Y
Custom	Y	Y	Y	Y
Note	Y	Y	Y	Y

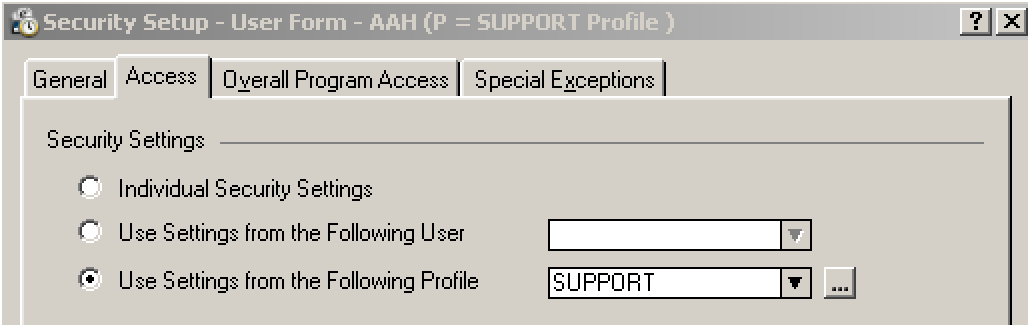
The most effective way to implement security is to set up Security Profiles. Security Profiles are a group of settings that can be applied to multiple users and thus avoids having to set security on an individual user basis.

Examples of Security Profiles might be ‘Partners’, ‘Attorneys’, ‘Support Staff’, ‘Accounting Staff’, or ‘Receptionist’.

The rights to view, add, change and delete any of the record types can be determined by the Security Profile assigned to the user.

Security can be set by record, by code, by staff, and by field. Care must be taken to avoid two negatives creating a positive or vice versa. And careful testing should be done to confirm the desired results have been attained.

Once a Security Profile is defined, simply go to the user record and assign it.



Security Settings

○ Individual Security Settings

○ Use Settings from the Following User

● Use Settings from the Following Profile SUPPORT