



DOCUMENT SECURITY CONTROLS

Presenting
**Managing the Assessment and Distribution of
Sensitive Documents**

January 23, 2006

LUCID IQ
428 S. Central Expressway
Dallas, Texas 75201
p. 214.221.9995
f. 214.221.9888
LUCIDIQ.COM

CONFIDENTIAL

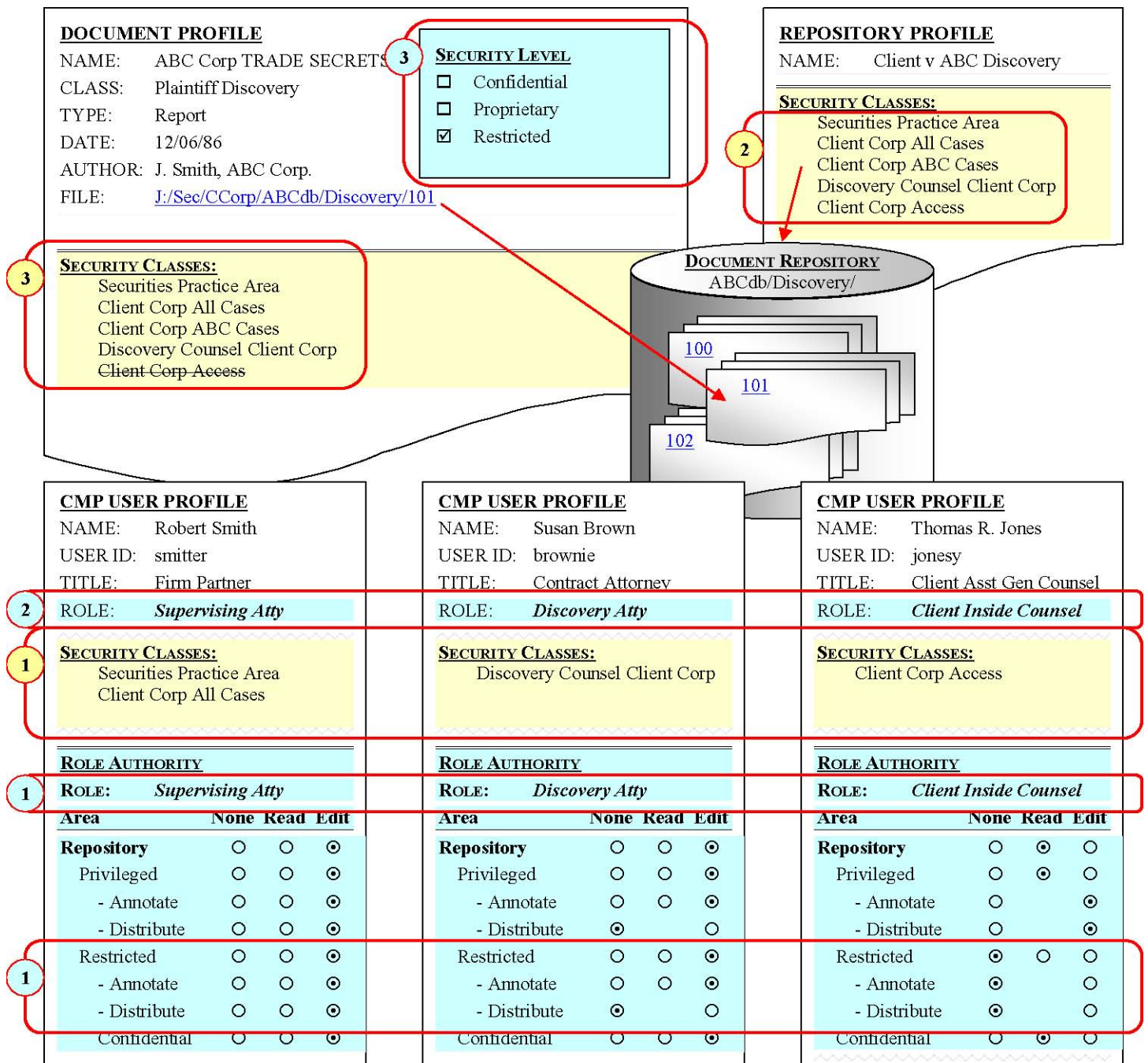
The contents of this document are confidential and are intended exclusively for the prospective customer of Lucid IQ designated above and its employees. Distribution or sharing of this information with persons or entities for which it is not intended is prohibited, in any form, without the express written consent of Lucid IQ.

DOCUMENT SECURITY CONTROLS

Managing the Assessment and Distribution of Sensitive Documents

This paper will address the management of sensitive documents in the context of both client and opposing party electronic document repositories for discovery and litigation support within the casemanagerpro ("CMPv3") application. Primarily relevant information is presented that is not intended to depict the full functionality of this aspect of CMPv3.

The figure below illustrates how records are identified and managed by associating security attributes to them. i) *Record Accessibility*, in this case either the repository or a document within it, is accessible by persons with one or more "Security Classes" assigned to them that match those of the record; ii) *User Ability* to view certain information or take specific actions within the record once it is accessed is based on the "Role" to which the individual is assigned. This provides a broad range of security management capabilities for the firm.



SECURITY CLASSES

Security Classes are simply created as a name and description. Applying these records is equally as simple – just assign them to various records as illustrated in the yellow highlighted areas of the figure above. If the particular record, whether it's a document or case or whatever, has an assigned class that matches one of the User's, access is granted. If not, it won't appear on their screen.

1. **User Security Class Access.** Each person that has access to the system has a User Profile that, among many other things, manages the rights the person has to see information and to act upon it. In Area 1 of the figure above, note that each member of this litigation team has different Security Classes assigned.

The Firm Partner has very non-restrictive settings, and every record in the Securities Area and all cases for Client Corp are accessible to him. Susan, as discovery counsel, can only open documents in the area marked for Discovery Counsel access for this case, and the Client can only open documents specifically classified for his access.

2. **Record Security Class Access.** As with all records, the Document Repository and the Document both have profiles that list all Security Classes assigned to individuals that may see them. Note the Repository includes i) the highest Security Class, i.e.: "Securities Practice Area", to which only senior personnel such as the partner are assigned, ii) the relatively restrictive "Discovery Counsel Client Corp" for the attorney that will likely never see anything other than discovery documents, and iii) "Client Corp Access" that allows the client into the Repository.

3. **Record Security Class Exclusion.** When the Document Record is created it may contain all of the settings of the Repository by default, so all three of our team members would have access.

First Defense: By deleting the "Client Corp Access" Security Class from the document profile, which is the only one assigned to Client Corp, the client will not be able to view the document, even if the link is emailed to them.

CMPv3 is intended to be used as a web-based system, so emailing documents should be shared for collaborative purposes and production via links to the database. Should the Discovery Attorney, or even the Partner, inadvertently send this document to the Client in a production set listing documents with link to the file the Client will be unable to view it.

ROLE AUTHORITY

Each User is assigned to a "Role" that is defined by the firm. Role information is highlighted in blue in the figure above. The Role definition controls i) whether a User can view certain information within a record to which they have access (per the Security Classes) and, if they can view it, ii) whether they can take some action such as editing or copying the record. Role definition allows the firm discretion to manage with some precision if desired, with over 300 manageable areas or actions, or at a higher level in less detail. As many Roles may be defined as necessary, and any number of people may be assigned to a single Role.

1. **Role Defined.** In the example above there are three Roles corresponding to the people involved in managing what we have termed "Restricted" Repositories and Documents. Note that the Supervising Attorney Role has highest authority; the ability to view and act on a Restricted Repository. A similar section would provide those same rights for Restricted Documents. The Discovery Attorney Role may Annotate but not Distribute. The Client Inside Counsel Role has Read (view only) access to Repositories (and Documents) generally, as well as Privileged. He does not have access even to read Restricted Documents.
2. **Role Assigned.** For each of the Users above a Security Role is assigned corresponding to their responsibilities.

3. **Users Managed.** If a Document is coded as Restricted, even if record-level Security Classes are not properly managed, the Discovery Attorney simply can not copy, print, or produce that record. Only the Supervising Attorney has been granted that authority.

Second Defense: By coding a document "Restricted" and establishing a Role that precludes distribution rights, the Discovery Attorney can not inadvertently or purposely produce the document for the client or anyone else.

The Client Inside Counsel has no ability to even view the document coded Restricted".

Third Defense: The Client Inside Counsel is not only restricted from viewing and editing the document, but does not even see evidence of it in the program or reports that he creates.

Additionally, if the Repository itself is restricted it could not be opened by the Client at all, thus protecting sets of Restricted Documents from disclosure either purposely or inadvertently.

Other methods of security or warning may be designed and created with relative ease, such as a pop-up warning that reads "WARNING: This Document is Restricted (or Confidential or Privileged)."

In summary, documents and sets of documents that should be protected from disclosure can be well managed. There are numerous methods by which a determined party could access such information, but a reasonable security policy for both physical and electronic management should provide a level of protection that well exceeds typical standards of conscientious firms.