INTRODUCTION

This document is designed as a supplement to the BDS Contacts & Companies for Contact Manager User Guide and the BDS Administrators Guide. It is designed as a discussion document for approaches to information control. It does not replace these Guides and the Guides remain the de facto reference source for all items discussed in this document.

OVERVIEW

BDS is designed as an 'open' system to make CRM information easily accessible to all users to encourage collaboration and effective leverage of information. There are therefore no restrictions on the records that users can access within an entity if they are granted access to that entity.

For example, a user who is granted access to the Contacts entity can access every contact record. That same user cannot access Experience records unless the user is specifically granted access to the Experience entity.

BDS recognizes however, the need to control visibility of certain field-level information that may be confidential or just not required and distracting to a user. In this situation Field Controls (FC) and Field-Level Security (FLS) can be enabled, together with User Security Rights (USR) to control access to fields for individual users and groups.

CONTROLLING ACCESS TO INFORMATION

Control and restriction of information to users is structured at the field level only. Record access (contacts and companies) cannot be restricted to specific users.

FIELD CONTROLS

Field Controls (FC) are set for each field individually for the overall control of the field. There are four FC options:

- Administrator
- Protected
- Required
- No Restrictions

Only one of these four controls may be applied to any single field. The control is enforced after the field is set to live. Access to and use of the field by individual users can be further restricted by FLS controls.
FIELD-LEVEL SECURITY

The Field-Level Security (FLS) controls are optional, and are not enforced until FLS is enabled for a field. There are three options:

- View/Edit
- View
- Hidden

One of these controls must be applied to all users and groups that have been granted access to the entity (Contacts, for example).

The default value is Hidden: when enabled, the value ensures the field is not visible to any users or Groups until the setting is changed.

The FLS can then be set to allow View and Edit permissions for specific users or groups. Note, however, the USRs attached to each User/Group at entity level also limit the permissions on the field.

Use FLS to override and increase the restriction on the Field Controls. A field that is FC "No Restrictions" can be made View-only for all users/groups, or even Hidden.

USER SECURITY RIGHTS

User Security Rights (USR) are applied to Users and Groups at entity level to control record and field access. The USR levels are:

- Guest – View only
- User – View/Edit
- Administrator – Admin rights

These USRs combine with the FLS to enable further restrictions on fields for specific users/groups.

For example:

FC = No Restrictions
FLS = View/Edit
USR = Guest is View only

PROFILES

Profiles provide an additional ‘screen’ or ‘tab’, within the General Profile as a means of partitioning and/or securing fields from different users and groups.

For example, perhaps only the billing fields are confidential and need to go into a Profile. Other fields may be of interest to only one group of users, such as Marketing or Administrators, so putting the marketing fields in a Profile aids easy navigation and prevents screen clutter for others users.

Profiles do not have inherent security to prevent access by any users/groups. However, the profile will not be visible for any users to select (or open) if the users’ FSL rights are set to Hidden for all the fields in the profile. If one field provides a user FLS View or above, then the user can call up the Profile. However, only the fields for which the user has FLS View rights will be visible.
Access to the Profiles is further controlled by USR. Only Users with User FSR can call up any Profile (providing it has a field for which they have View FLS). This is because Profiles are accessed in Edit mode for the individual record so only USR User and Admins can access and select them.

Guest USR users cannot call a profile because they do not have Edit rights for records in the entity. They can open a profile only after it has been set by another user. They can view the fields for which they have FLS View rights. If there are no populated fields for which they have FLS View rights in the profile, then the profile is greyed out and cannot be opened.

USERS AND GROUPS

The use of Groups simplifies adding large numbers of users to (the same) USRs and adding users to FLS settings.

It can be complex to maintain the increasing granularity of Groups—down to one or two users—to reflect a tier of staff in a specific practice in a particular record. In these cases, applying individual users to FLS or publishing of lists might be easier to manage. This needs to be considered on a case-by-case basis.

USE CASE 1. CONFIDENTIAL INFORMATION

Confidential information can be hidden from users and made available to others using a combination of Field-Level Security and Groups.

SAMPLE USE CASE

Assume, for example, a firm with two offices, London and Hong Kong. Both offices want to keep their local client billing figures, presented in the BDS Company records, private and confidential to the respective office Partners.

In this case, a separate set of billing fields are created for each office:

- A Group is created for London Partners, and the Field-Level Security is set to provide the Group with View-only access to these fields.
- A Hong Kong Partners Group is also created and given View-only access to their billing fields.

The result of these settings is that the partners and staff in one office cannot view billing fields for the other office because they have not been granted access.

Let’s also assume that the global CFO needs to view and edit the billing figures for both offices. The CFO is therefore granted Field-Level Security permissions to edit the billing fields of both offices.

If the London and Hong Kong offices have their own billing fields, these fields could be assigned to separate Profiles, specific to each Office.
USE CASE 2. PUBLISHING INFORMATION TO USERS

Contact Lists and Saved Searches in any entity can be published to users to streamline their access to information.

- Lists and Saved Searches can be published to Users individually or to Groups of users.
- Contact Lists can be published to OLC users in groups or individually. Saved Searches, however, are not available to OLC users.

SAMPLE USE CASE

Assume that Marketing sends newsletters and runs events for two very different types of users:

- On behalf of complete practices, such as M&A Trends, on a global basis
- Very local events on Employment law changes in a country or city where the firm has a small office.

Marketing therefore wants to publish these marketing lists to different sets of Partners in their OLC toolbar for convenience.

- For the global M&A Trends Newsletter, the new subscriber list can be published to the Group "M&A Partners – Global".
- For the employment law event in Madrid, there is only one partner and one associate. The list is therefore published to them as individuals.