

USER ACCESS & ROLES IN THE APPLICATION

Purpose of this Document

- ✓ Provides guidance on user roles, permissions, and access control within the application.
- ✓ Ensure structured access by assigning users to groups, defining roles, and setting confidentiality levels.
- ✓ Helps users navigate their responsibilities efficiently while maintaining security and compliance.

USER ROLES

Users within the application are assigned to one or more roles, which determine their access and permissions. The system consolidates the permissions from all assigned roles to form a single security profile for each user.

- Users can hold multiple roles within an organization.
- Permissions from various roles are combined into a single security profile.
- **User Permission Roles** are managed exclusively by **Teessen Consulting** and cannot be modified by users or System Administrators.

USER GROUPS

Users can be linked to multiple groups, granting them access to relevant company and person records.

Groups function as a segmentation mechanism, ensuring controlled access.

User Groups are directly linked to Contact Groups – always ensure users are appropriately linked when a new Contact Group is created.

CONFIDENTIALITY LEVELS

Confidentiality settings restrict access to sensitive information based on predefined levels.

- Levels range from “None” to “Level 5”, controlling document, note and task access.
- A user with “Level 3” access can only view information classified at Level 3 or lower.
- This feature enhances security by ensuring data visibility is role appropriate.

BEST PRACTICES:

To optimize security and efficiency, follow these best practices:



Regularly review user roles and permissions: To ensure compliance with organizational needs.



Ensure users are correctly linked to the appropriate Contact Groups: To prevent access issues.



Assign appropriate confidentiality levels: to sensitive information for enhanced security.

For further assistance, refer to the **Help Section** or contact **Teessen Consulting Support**.