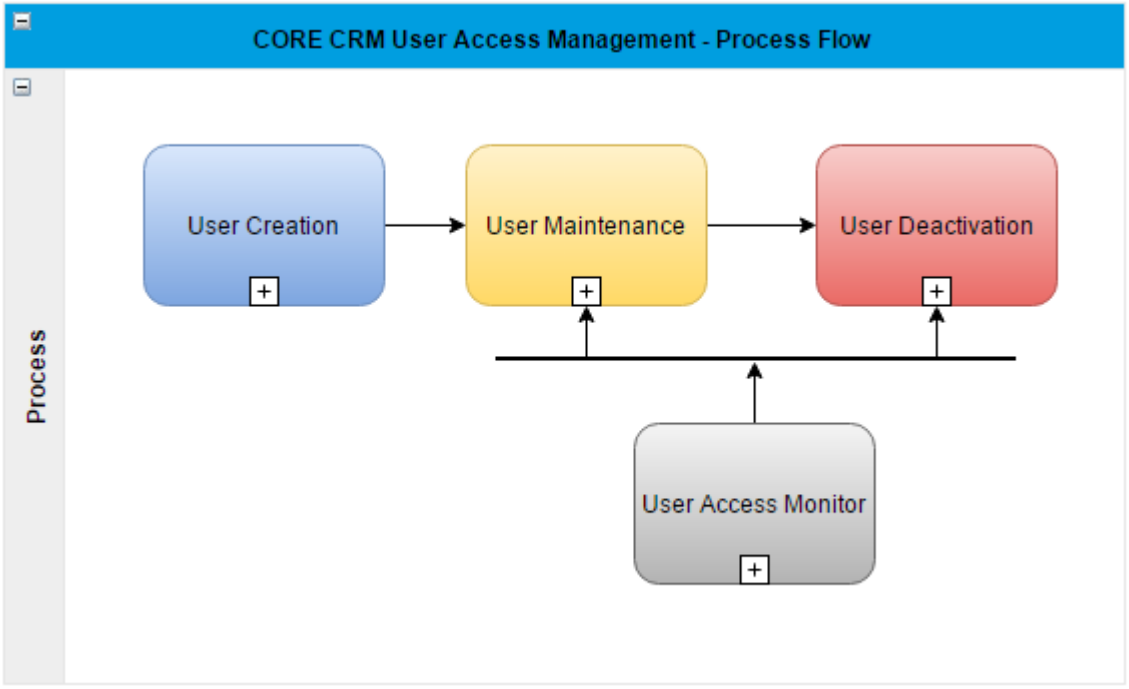
SpP Access Management

Objective and Scope

CRM Access management is the process of granting authorized users the right to use CRM ICARe Application, while restricting access to non-authorized users. This Section aims to describe how SpP User Access management is managed by IS CRM team according to **Solvay Information Security Policies** and GBU Guidelines, this Process applies to:

- ICARe Salesforce.com IS solution
- IT users: both Solvay internal employees working for IS and external IT subcontractors
- Access configurations will give access to :
  - ICARe CRM data

Table of Contents



Key Roles and Responsibilities

Abb	Definitions
CRM	Customer Relationship Management system

- **User direct manager** Direct manager of the user, responsible to request the access request or Removal to CORE CRM.
- **GBU User Responsible** Person in the GBU in charge of centralizing and creating the IS request, can be the Data Steward, CRM Champions, listed in CORE CRM Key User List
- **IS CRM Build - Security team** Team in charge of maintaining the authorization concept for the CRM of the Solvay Group in All Environments.
- **IS CRM Adoption team** Team in charge of Critical Users /Access Daily Operations in PROD and UAT Environments.
- **IS CRM Support (CGI)** External Provider team in charge of Access Management Daily Operations in PROD and UAT Envir onments

SBS	Solvay Business Services
IS	Information Services
GBU	Global Business Unit
Freshdesk	Ticketing system used for IS tickets management
GUDsis	Global User Database Solvay information services
SISO	Solvay Information Security Organization

Key Principles

CORE CRM User Access Management Process will be managed following the key principles:

- Any request related to Users, has to be initiated by the User's direct manager or GBU User Responsible.
- The User's direct manager is in charge of reporting any kind of change related to the user that can have an impact on access rights: change of job, leaving, retirement.
- All Requests should be record in IS Ticketing System, Freshdesk.
- **All Data Access requests (CORE CRM and Qlikview) needs to be approved by GBU Responsible of that Data.**
- Accesses are defined on the basis of GBU/Jobs and maintained by IS CRM Build - Security team that updates the CORE CRM Access Matrix and IS CRM Support (CGI) creates / modifies / removes Users accesses in accordance with the information provided in this Matrix.
- As stated by CISO rules, IT users should have only display accesses in the Production environment. However IT users involved in the Application support or in project implementation need also creation/modification accesses. In order to mitigate risks due to these privileges, in the Production system of the CRM we have available the audit trail report.
- Critical Accesses will be monitored as Described in Section User Access Monitor.
- User Mass creation (during projects, roll-out for example) follow a fast-track process.
- User creation in CORE CRM should only be implemented after User is created in GUDsis.
- External users access:
  - should be identified with "-ex", "-ext", "-exterieur" or "-contractor" at e-mail address or username.
  - end date for the access is mandatory.
- Generic email address are forbidden, but if no other way:
  - email owner approval is mandatory.
  - end date for the access is mandatory, after each complete year of use, password should be changed.

Overall Process Description

User Creation

Is considered a New User in CORE CRM when, there is no Active user Account for that user's email address. User creation request can be requested for a User to have:

- **Access to one GBU** - User creation request should be created by the GBU User Responsible via Freshdesk. The request should be validated by IS CRM Support team according to CORE CRM Access Matrix, and additional approvals might be required before proceeding with Operational Procedure 'CORE CRM User Creation'
- **Access to Multi-GBU**: Is an access to several GBU data (Salesforce and Qlikview), only Champions/Data Steward are authorized to request access to more than one GBU. User creation follows the same Operational Procedure 'CORE CRM User Creation' and then user will be added to the correspondent Public Groups to get the access to the authorized data.

User Maintenance

Is considered User Maintenance in CORE CRM when, a request refers to an existing Active or Inactive User Account, we can have the following scenarios, and as per point 3. Review of 08_Access_Control_Policy_V1.0 of Solvay Information Security Policies:

- **Transfer to another Solvay GBU**: Existing User that will terminate activities for one GBU A and start Activities to another GBU B, this type of transference requires a transition phase where User should have access to both GBUs data. Due to Data Visibility concerns, during the transition period User will keep GBU A access User Account and a new User Account for GBU B access should be created, IS CRM Support team can proceed with Operational Procedure User Transference Between GBUs

Additionally, IS CRM Support team will monitor user transference to another GBUs as described in section Access Monitor.

- **Transfer inside same GBU** (job change that still allows access to CORE CRM otherwise see section User Deactivation): User Maintenance r equest should be created by the GBU User Responsible via Freshdesk. The request should be validated by IS CRM Support team according to CORE CRM Access Matrix, and additional approvals might be required before proceeding with requested User Account Configurations update.

- **Extend User Access to another GBU** (Access to Multi-GBU): For an existing Active User that should keep current GBU access and have his scope extended to another GBUs. User access extension request should be created by the GBU User Responsible via Freshdesk. The request should be validated by IS CRM Support team according to CORE CRM Access Matrix, and additional approvals might be required before proceeding with requested User Access Extension configurations.
- **Re-activate Inactive User Account**: Requests for which there is an inactive account for the user email address, IS CRM Support team should evaluate in which of the previous scenarios the request is referring to, and proceed as described. If end user reports via freshdesk an access issue that requires User Account re-activation, IS CRM Support team needs to contact GBU User Responsible for approval.

User Deactivation

GBU User Responsible is responsible to request User deactivation via Freshdesk for:

- End of Contract with Solvay
- Change of Jobs that CORE CRM system access is not required or forbidden (example: from Sales to Procurement).
- Other reasons.

IS CRM Support team should proceed with Operational Procedure 'CORE CRM User Deactivation'

Additionally, IS CRM Support team will monitor User leaving solvay and not logging in for more than 3 months as described in section Access Monitor.

User Access Monitor

- **No log in in the past 90 days:** As per point 3. of 08_Access_Control_Policy_V1.0 of Solvay Information Security Policies, and additionally to the Operational Procedures defined in this Document, IS CRM Support team will perform on a monthly basis the procedure to identify Users who haven't logged in the past 90 days and contact them to inform that their Account will be disabled, this will also free Application licenses.

- **Identification of Solvay Inactive Users:** As per point 3. of 08_Access_Control_Policy_V1.0 of Solvay Information Security Policies, and additionally to the Operational Procedures defined in this Document, and also with the aim to free Application Licences, IS CRM Support team will perform 2 Procedures:

    - CORE CRM GUDsis Service Upload - to be performed on a Monthly basis
    - CORE CRM Identification of Solvay Inactive Users - Performed on a Daily basis - as been Automated: a daily program is running on GUDsis application to send the list of Solvay Inactive Users to CRM Support mailbox sbs-is-crm.support@solvay.com and automatically a ticket in freshdesk for User deactivation is created, IS CRM Support team can proceed with Operational Procedure 'CORE CRM User Deactivation '

- **Monitor User transference from One GBU to another GBU**
    - Procedure under construction

- **Critical Access:** As per point 3. of 08_Access_Control_Policy_V1.0 of Solvay Information Security Policies, and additionally to the Operational Procedures defined in this Document, IS CRM Support Team / IS CRM Build team will perform at least once a year and whenever is necessary:

Critical Access	Procedure
System Administrator Profile	Procedure under construction
Export Reports	Procedure under construction
View All Data	Procedure under construction
Modify All Data	Procedure under construction

Authorizations & Roles

Author(s)	Verification	Approval
Julien Gasqueton (Security Lead)	Julien Gasqueton (Security Lead)	CRM Domain Leader
xx/xx/20xx	xx/xx/20xx	xx/xx/20xx

Version Control

Version	Date	Description
00	xx/xx/20xx	Draft Version

Reference Documents
03_Personnel_Policy_V1.0
08_Access_Control_Policy_V1.0
11_EndUser_Security_Policy_V1.0