

<b>Number:</b>	05.1.5	<b>Page:</b>	1 of 2
<b>Latest Version:</b>	1.0	<b>Revision Date:</b>	12/10/2015
<b>Effective Date:</b>	03/28/2016	<b>Replaces:</b>	NEW
<b>Revised By:</b>	Joshua Graves	<b>Review Cycle/Date:</b>	Annual
<b>Reviewed By:</b>	Amy Max	<b>Reviewing Unit:</b>	Service Desk
<b>Title:</b>	Confidential/Regulatory Information in CRM Cases Standard		
<b>Description:</b>	This document is the operating standard for Confidential/Regulatory Information in CRM Cases.		

## Confidential/Regulatory Information in CRM Cases Standard

1. General Statement of Purpose
  - 1.1. Confidential/Regulatory Information must not be listed in a CRM Case.
2. Scope
  - 2.1. This standard covers the steps to protect all customers' Confidential/Regulatory Information in CRM Cases.
3. Discipline
  - 3.1. Service Management
4. Terms and Definitions
  - 4.1. Confidential/Regulatory Information – (1) Any information that can be used to verify or trace an individual's identity, such as a PIN, password, partial or entire social security number, date and place of birth, mother's maiden name or biometric records; or (2) any information that is controlled by a regulatory body, such as medical, educational, financial, credit card and federal tax information.
5. Instructions
  - 5.1. **Confidential/Regulatory Information must not exist in CRM Cases.**
  - 5.2. If a customer calls in to the OMES Service Desk, Service Desk Technicians are prohibited from documenting any Confidential/Regulatory Information in the CRM Case.
  - 5.3. If the OMES Service Desk notices Confidential/Regulatory Information in a CRM Case generated automatically from a customer email or from the Customer Portal, they must delete the information and document the incident in the case.
  - 5.4. If the Service Provider receives a CRM Case with Confidential/Regulatory Information in it, they must delete the information and document the incident in the case. Typically, if the Service Provider finds Confidential/Regulatory Information in a case, it would have come from a customer's email. After deleting the Confidential/Regulatory Information, the Service Provider must create a CRM Case to have the Service Desk delete the original email from the Service Desk email history.
    - 5.4.1. The Service Provider can identify cases where content was submitted via email by looking under Step 1 in the CRM Case. The Call Source dropdown will show "E-mail".
  - 5.5. If Confidential/Regulatory Information is discovered in the Journal Entries, a CRM Case must be created and sent to the OMES Service Desk. The OMES Service Desk will delete the Journal Entry containing the information.

<b>Number:</b>	05.1.5	<b>Page:</b>	2 of 2
<b>Latest Version:</b>	1.0	<b>Revision Date:</b>	12/10/2015
<b>Effective Date:</b>	03/28/2016	<b>Replaces:</b>	NEW
<b>Revised By:</b>	Joshua Graves	<b>Review Cycle/Date:</b>	Annual
<b>Reviewed By:</b>	Amy Max	<b>Reviewing Unit:</b>	Service Desk
<b>Title:</b>	Confidential/Regulatory Information in CRM Cases Standard		
<b>Description:</b>	This document is the operating standard for Confidential/Regulatory Information in CRM Cases.		

5.6. Any violations in the process of securing Confidential/Regulatory Information should be reported to the IS-OMES Security team by CRM Case immediately upon discovery. The Security team will need to know who is involved and what type of information was involved in the violation.

## 6. Roles and Responsibilities

### 6.1. Service Desk Technician

- 6.1.1. Does not put any Confidential/Regulatory Information in CRM Cases.
- 6.1.2. Deletes any Confidential/Regulatory Information found in a CRM Case and documents the case.
- 6.1.3. Deletes any email in the Service Desk email history that contains Confidential/Regulatory Information.

### 6.2. Service Provider

- 6.2.1. Deletes any Confidential/Regulatory Information found in a CRM Case and documents the case.
- 6.2.2. Creates a CRM Case for the OMES Service Desk when they find Confidential/Regulatory Information in a CRM Case.