

## Management System: Information Resource Management

### Subject Area: Computer Systems Management (Including Help Desk)

### Procedure: 3 - Requesting User Accounts for Visitors (Non-EMCBC Employees)

Issue Date:  
9/4/2012

Lead Subject Matter Expert:  
Philip LaGamba

Management System Owner:  
Ward Best

#### 1.0 Applicability

This procedure applies to all visitors requiring access to the Environmental Management Consolidated Business Center (EMCBC) Information Systems. A visitor (non-EMCBC employee) is any individual who is not based at the EMCBC or the attached sites but requires [General Access](#) to the EMCBC system to accomplish their job function.

#### 2.0 Required Procedure

The purpose of this procedure is to establish the process for requesting user accounts, rights, and access to specialized applications for visitors (non-EMCBC employees). These accounts are managed similarly to those for EMCBC employees with the following difference: the Rules of Behavior for EMCBC Information Systems (User Agreement) **must be signed by the Federal Sponsor who must indicate the expected end date for the account as well as the specific rights required for the user.**

<b>Step 1</b>	The EMCBC-based Federal Sponsor notifies the Office of Information Resource Management (OIRM) of the need for the visitor account, including end date, and any known <a href="#">Special Access</a> rights using the <a href="#">Computer Service Request</a> (CSR) system. For instructions on CSR, see Procedure 1, Computer Service Request (CSR).  <b>NOTE: The CSR system is used only to generate the account; the account will not be enabled without the completed Rules of Behavior for EMCBC Information Systems (User Agreement).</b> In most cases, the visitor will not be available to complete the User Agreement until after the Start Date.
<b>Step 2</b>	Visitor completes Pages 1-3 of the Rules of Behavior for EMCBC Information Systems ( <a href="#">User Agreement</a> ) and submits to Federal Sponsor to complete Page 4 (Additional Specific Access Rights for EMCBC Drives, Systems and Applications).  <b>NOTE: If Remote Access Connection service is required, visitor fills out the <a href="#">User Acknowledgement Agreement (UAA) for Two-Factor Authentication and Remote Access Connection Services</a> and hand-carries to OIRM for identity proofing. After</b>

	verification, token is issued.
<b>Step 3</b>	Once the User Agreement is completed, the Federal Sponsor <b>signs</b> and submits it to OIRM.
<b>Step 4</b>	OIRM verifies information, creates new date-limited account, and provides visitor with credentials.
<b>Step 5</b>	Visitor logs in and completes <a href="#">Cyber Security Training</a> within 30 days.
<b>Step 6</b>	OIRM sets end-date on account and files the completed User Agreement.
<b>Step 7</b>	OIRM logs activity in IM Maintenance Log, as applicable.

### 3.0 References

- IMP-8308-001 – *Cyber Security – Account Management and User Responsibilities*
- [Procedure 1 – Computer Service Request](#)

### 4.0 Records Generated

Records generated through implementation of this procedure are identified as follows and are maintained by the Office of Information Management in accordance with the EMCBC Organizational File Plan.

<b>Records Category Code</b>	<b>Records Title</b>	<b>Responsible Organization</b>	<b>QA Classification (Lifetime, Non-Permanent or N/A)</b>
ADM 01-29.2-A3	Administrative Training Records – Cyber Security Training	Office of Information Management	N/A
GRS 24-03-B1	IT Asset and Configuration Management Files – User Agreements, Requests for User Accounts	Office of Information Management	N/A
GRS 24-08-C	IT Operations Records – Information Management Maintenance Log	Office of Information Management	N/A