



January 7, 2014

Via Electronic Mail to: gwinterhalter@epmsolutions.com

Mr. Greg Winterhalter
EPM Solutions, LLC
2440 Camino Ramon, Suite 275
San Ramon, CA 94583

Re: FOIA FY 14-04

Dear Mr. Winterhalter:

Pursuant to your request for information under the District of Columbia Freedom of Information Act ("FOIA") received December 2, 2013, please find attachments and the below responses to address your questions regarding the Request for Quotation to Build & Implement SharePoint 2010 Intranet dated April 13, 2012.

1. Awarded Proposal to RFQ: Build & Implement SharePoint 2010 Intranet dated April 13, 2012.

This solicitation was cancelled so a contract was not awarded.

2. Copy of IT or organization Security Policy to protect sensitive data access to SharePoint documents or Project Server data or general consultant access to organization information.

The DCRB Policy governing Personally Identifiable Information is attached. This policy is used to protect sensitive data access to SharePoint documents, Project Server data, or general consultant access to organization information.

3. Copy of any recent successful proposal requiring vendor to respond to similar security for DCRB-14-010, page 18, paragraph F.

In response to solicitation number DCRB-14-006 for FileNet Maintenance and Support Services, Document Access Systems ("DAS") Incorporated submitted a successful proposal that is attached hereto. However, the DAS Information Security Policy and Standards was omitted since it contained proprietary and confidential information. Such information is exempt from disclosure pursuant to D.C. Official Code § 2-534(a)(1). This FOIA exemption code states: "Trade secrets and commercial or financial information obtained from outside the government, to the extent that

disclosure would result in substantial harm to the competitive position of the person from whom the information was obtained."

4. The winning proposal from Projility, Inc. to implement Project Server 2010 completed from Nov 24, 2010 to May 17, 2011 or earlier.

Pursuant to the Office of the Chief Technology Officer's ("OCTO") arrangement with Projility, DCRB prepared a Statement of Work for Projility to perform services as outlined in the attached agreement dated June 29, 2010.

5. The RFP to Implement Project Server 2010 completing from Nov 24, 2010 to May 17, 2011 or earlier.

If an RFP existed, OCTO would have solicited for these services. DCRB does not have the RFP.

6. Projilty's project deliverable documents delivered to DCRB in the course of its contract.

Projilty's project deliverable documents are attached.

Please know that, under D.C. Official Code § 2-537 and 1 DCMR 412, you have the right to appeal this letter to the Mayor or to the Superior Court of the District of Columbia. If you elect to appeal to the Mayor, your appeal must be in writing and contain "Freedom of Information Act Appeal" or "FOIA Appeal" in the subject line of the letter as well on the outside of the envelope.

The appeal must include (1) a copy of the original request; (2) a copy of any written denial; (3) a statement of the circumstances, reasons, and/or arguments advanced in support of disclosure; and (4) a daytime telephone number, and e-mail and/or U.S. Mail address at which you can be reached. The appeal must be mailed to: The Mayor's Correspondence Unit, FOIA Appeal, 1350 Pennsylvania Avenue, N.W., Suite 316, Washington, D.C. 20004. Electronic versions of the same information can instead be e-mailed to The Mayor's Correspondence Unit at foia.mayor@dc.gov.

Further, a copy of all appeal materials must be forward to me as the DCRB Freedom of Information Officer. Failure to follow these administrative steps will result in delay in the processing and commencement of a response to your appeal to the Mayor.

Sincerely,



Erie F. Sampson
General Counsel/FOIA Officer

DCRB
PERSONALLY IDENTIFIABLE
INFORMATION POLICY



Information Technology

District of Columbia Retirement Board

Personally Identifiable Information Policy

in compliance with ISO 20000

August 28, 2013
Version 1.0

DCRB IT- Policy		
Title: Personally Identifiable Information Policy	Reference: BS ISO IEC 20000-2 6.6, BS ISO/IEC 27001:2005, BS 27005-2:2008	Version 1.0
Issued By: DCRB IT Security	Approved By: DCRB Director of Information Technology	

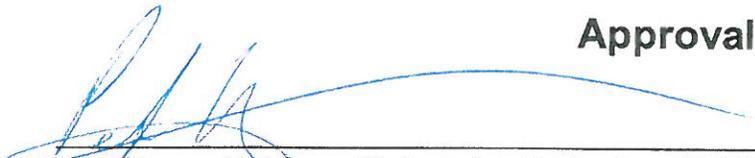
Table of Contents

1.0	Purpose	3
2.0	Scope	3
3.0	Policy	3
4.0	Policy Enforcement	5
5.0	Policy Owner	5
6.0	Policy Review	5
7.0	Policy References	5

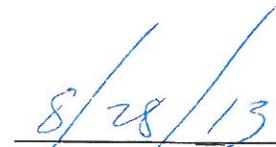
Revision History

Version	Description of Change	Author/Reviewer	Date
0.1	Technical Authoring	Clay Pendarvis	8/14/13
0.2	Knowledge Editing	Tony Phan Ferdinand Frimpong Mark Bojeun	8/16/13
0.3	Review of Knowledge Editing	Tony Phan Mark Bojeun	8/16/13
0.4	Language Edit and Layout Editing	Justin Baker	8/19/13
0.5	Review of Language and Layout Editing	--	--
0.6	Management Editing	Leslie King	8/27/13
0.7	Review of Management Editing	Justin Baker	8/28/13
0.8	Final Editing	Justin Baker	8/28/13
1.0	Delivery	Peter Dewar	8/28/13

Approval



 Peter Dewar, Director of Information Technology, DCRB



 Date

DCRB IT- Policy		
Title: Personally Identifiable Information Policy	Reference: BS ISO IEC 20000-2 6.6, BS ISO/IEC 27001:2005, BS 27005-2:2008	Version 1.0
Issued By: DCRB IT Security	Approved By: DCRB Director of Information Technology	

Personally Identifiable Information Policy

1.0 Purpose

DCRB information technology (IT) recognizes its need to maintain the confidentiality of personal identifiable information (PII) and understands that such information is unique to each individual. This policy addresses PII that is managed and produced from various types of DCRB work activities and applies to DCRB employees, contractors, consultants, and vendors, including PII maintained on the DCRB customer base (District of Columbia teacher, police, and firefighter retirees).

2.0 Scope

The scope of this policy is intended to be comprehensive and includes requirements for the security and protection of PII throughout the agency and its approved vendors both onsite and offsite. All applicable DCRB departments will develop and implement specific processes and procedures for protecting PII when necessary. Such policies will be governed by applicable District of Columbia and Federal laws. These laws govern in the event of any conflict between these laws and DCRB policies.

3.0 Policy

In the DCRB organizational environment, PII is unique, personal data that includes, but is not limited to, the following:

- Social Security Numbers (or their equivalent issued by governmental entities outside the United States)
- Employer Identification Numbers (or their equivalent issued by government entities outside the United States)
- State or foreign driver's license numbers
- Date(s) of birth
- Government or individually held credit or debit transaction card numbers (including PIN or access numbers) maintained in organizational or approved vendor records

PII may reside in hard copy or in electronic records; both forms of PII fall within the scope of this policy.

3.1 Vendors

Individual(s) or companies that have been approved by DCRB as a recipient of organizational and member PII and from which DCRB has received certification of their data protection practices that conform to this policy. Vendors include all external providers of services to the agency as well as proposed vendors. No PII can be transmitted to any vendor in any method unless the vendor has been pre-certified for the receipt of such information.

3.2 PII Retention

DCRB IT- Policy		
Title: Personally Identifiable Information Policy	Reference: BS ISO IEC 20000-2 6.6, BS ISO/IEC 27001:2005, BS 27005-2:2008	Version 1.0
Issued By: DCRB IT Security	Approved By: DCRB Director of Information Technology	

DCRB understands the importance of minimizing the amount of PII it maintains and will retain PII only as long as necessary. A joint task force comprising members of the DCRB Legal, Finance, IT, Contracts and Human Resources Departments will maintain organizational record retention procedures, which will dictate the length of data retention and data destruction methods for both hard copy and electronic records.

3.3 PII Training

All employees and contractors at DCRB who may have access to PII will be provided with introductory training regarding PII policy, will be provided a copy of this PII policy, and will be provided a copy of PII-related procedures for the department to which they are assigned. Employees in positions with regular ongoing access to PII or those transferred into such positions will be provided with training that reinforces this policy and reinforces the procedures for the maintenance of PII. Employees will receive annual training regarding the security and protection of PII and company proprietary data

3.4 PII Audit(s)

DCRB will conduct audits of PII maintained by DCRB in conjunction with fiscal year closing activities to ensure that this PII policy remains strictly enforced and to ascertain the necessity for the continued retention of specific PII throughout DCRB. Where the need no longer exists, PII will be destroyed in accordance with protocols for destruction of such records and logs will be maintained that record the dates of the specific PII destruction. The audits will be conducted by the DCRB Finance, IT, Procurement, and Human Resources Departments under the auspices of the DCRB Legal Department.

3.5 Data Breaches/Notification

Databases or data sets that include PII may be breached inadvertently or through wrongful intrusion. Upon becoming aware of a data breach, DCRB will notify all affected individuals whose PII may have been compromised, and the notice will be accompanied by a description of action being taken to reconcile any damage as a result of the data breach. Notices will be provided as expeditiously as possible and will be provided no later than the commencement of the payroll period after which the breach was discovered.

3.6 Data Access

DCRB maintains multiple IT systems in which PII resides; thus, user access to such IT resources will be the responsibility of the DCRB IT Department. The DCRB IT Department will create internal controls for such IT resources to establish legitimate access for users of data, and access will be limited to those users approved by IT. Any change in vendor status or the termination of an employee or contractor with access to PII will immediately result in the termination of the user's access to all systems where the PII resides.

3.7 Data Transmission and Transportation

1. Within DCRB: DCRB will have defined responsibilities for onsite access of data that may include access to PII. DCRB IT Security will have oversight responsibility for all electronic records and data access to those electronic records. DCRB will be responsible for implementing the access and terminating the access of individual users to PII within the organization and providing timely notice to IT.

DCRB IT- Policy		
Title: Personally Identifiable Information Policy	Reference: BS ISO IEC 20000-2 6.6, BS ISO/IEC 27001:2005, BS 27005-2:2008	Version 1.0
Issued By: DCRB IT Security	Approved By: DCRB Director of Information Technology	

2. Agencies and Vendors: DCRB may share data with other agencies and vendors such as the Office of Personnel Management, the U.S. Department of the Treasury, and the DCRB independent actuary who have legitimate business needs for PII data. Where such sharing of data is required, the DCRB IT Department will be responsible for creating and maintaining data encryption and protection standards to safeguard all PII during transmission to those agencies and vendors. An approved vendor list will be maintained by the DCRB Procurement Department, which will be responsible for notifying DCRB IT of any changes to vendor status.

3. Portable Storage Devices: DCRB will reserve the right to restrict the PII it maintains in the workplace. In the course of doing business, PII data may also be downloaded to laptops or other computing storage devices to facilitate agency business. To protect such data, the agency will require that those devices use DCRB IT Department-approved encryption and security protection software while such devices are in use on or off company premises. The DCRB IT Department will be responsible for maintaining data encryption and data protection standards to safeguard PII that resides on these portable storage devices.

4. Off-Site Access to PII: DCRB understands that employees may need to access PII while off site or on business travel, and access to such data shall not be prohibited subject to the provision that the data to be accessed is minimized to the greatest degree possible while still meeting business needs and that such data shall reside only on assigned laptops/approved storage devices that have been secured in advance by the DCRB IT Department with data encryption and data protection standards.

4.0 Policy Enforcement

Failure to follow this policy may result in disciplinary action and/or contract termination.

5.0 Policy Owner

DCRB IT Security is responsible for this policy.

6.0 Policy Review

This policy will be reviewed annually by DCRB IT management. All employees, contractors, consultants, and vendors will review this policy, and will acknowledge in writing that they have read this policy.

Issue Date of Policy: February 2013

Next Management Review Date: February 2014

7.0 Policy References

- ISO 20000
- Information Technology Infrastructure Library (ITIL) standards
- DCRB IT Information Security Policy (February 15, 2013)
- DCRB Employee Handbook (November 2012)

**DAS RESPONSE TO RFP FOR
FILENET MAINTENANCE AND
SUPPORT AMENDMENT**

“DESCRIPTION OF AMENDMENT/MODIFICATION,”

Request for Proposal for FileNet Maintenance and Support Services is amended as described herein.

N. Security and Background Checks

Offeror shall provide a risk mitigation plan, including but not limited to, the processes employed by the Offeror to provide data and personnel security in compliance with Privacy Act of 1974, 5 U.S.C. § 552a, and the Department of the Treasury’s system of records notice TREASURY/DO .214 Fed Reg. 46284 (2005). The Offeror shall provide as part of the risk mitigation plan how it will meet the requirements of DCRB’s Personally Identifiable Information (PII) Policy included as Appendix A by providing the following:

- A list of the anticipated threats and hazards that the contractor must guard against;
- A description of the safeguards that the contractor must specifically provide; and
- Requirements for a program of Government inspection during performance of the contract that will ensure the continued efficacy and efficiency of safeguards and the discovery and countering of new threats and hazards.

DAS Response: DAS has a risk mitigation plan meets or exceeds the requirements as set forth in the amendment/modification. See Attachment A – DAS Risk Mitigation Plan for DCRB FileNet Maintenance and Support Services.

**RISK MITIGATION PLAN FOR
FILENET MAINTENANCE AND
SUPPORT SERVICES**

SOW



Risk Mitigation Plan for FileNet Maintenance and Support Services

STATEMENT OF WORK



DOCUMENT ACCESS SYSTEMS
Enterprise Content Management

November 8, 2013

TABLE OF CONTENTS

Proprietary Notice 3

1.0 Introduction 4

2.0 Threat and Hazard Identification 4

3.0 Safeguards 4

4.0 DCRB Inspection 4

5.0 Security Contacts 5

 5.1 District of Columbia Retirement System Key Personnel 5

 5.2 DAS Key Personnel 5

Proprietary Notice

This document contains confidential information of Document Access Systems, which is provided for the sole purpose of permitting the recipient, District of Columbia Retirement System (DCRB), to evaluate the plan submitted herewith. In consideration of receipt of this document, the recipient agrees to maintain such information in confidence and not to reproduce or otherwise disclose this information to any person outside the group directly responsible for evaluation of its contents.

This plan has been prepared in accordance with accepted techniques for risk mitigation and Document Access Systems' understanding of your requirements based on the information provided to us by District of Columbia Retirement System. All values, charts, designs and related information contained in this proposal reflect Document Access Systems best practices based on this information.

1.0 Introduction

Document Access Systems (DAS) provides ongoing FileNet Maintenance and Support services to the District of Columbia Retirement Board. In accordance with applicable laws and regulations, DAS must provide a risk mitigation plan, including but not limited to, the processes employed to provide data and personnel security in compliance with Privacy Act of 1974, 5 U.S.C. § 552a, and the Department of the Treasury's system of records notice TREASURY/DO .214 Fed Reg. 46284 (2005). DAS must provide as part of the risk mitigation plan how it meets the requirements of DCRB's Personally Identifiable Information (PII) Policy by providing the following:

- A list of the anticipated threats and hazards that DAS must guard against;
- A description of the safeguards that DAS must specifically provide; and
- Requirements for a program of Government inspection during performance of the contract that will ensure the continued efficacy and efficiency of safeguards and the discovery and countering of new threats and hazards.

This plan conforms to DAS Information Security Policy and Standards effective July 1, 2013 (attached).

Note that this risk mitigation plan applies solely to the services DAS provides as part of the FileNet Maintenance and Support services and does not include DCRB infrastructure and other IT applications and services for which DAS does not have responsibility.

2.0 Threat and Hazard Identification

DAS has identified the following threats and hazards as they pertain to the FileNet Maintenance and Support services provided.

- Unauthorized access via VPN
- Authorized access via VPN by personnel who do not pass required background checks
- Unsecured access by DAS personnel
- Release of PII to unauthorized personnel

3.0 Safeguards

The following safeguards are in place to ensure DAS guards against the identified threats and hazards.

- All DAS personnel will comply with DAS Information Security Policy and Standards effective July 1, 2013 (attached).
- If required by DCRB, DAS will perform background checks on all personnel with authorized access to DCRB systems.
- Only personnel with a demonstrated need will be granted access to DCRB systems.
- Access to DCRB systems will be via DCRB VPN only
- DAS will not store or process any DCRB data on DAS or DAS controlled equipment or systems.
- DAS personnel will not release VPN access credentials to unauthorized personnel.

4.0 DCRB Inspection

DAS will provide, at DCRB cost, a program of Government inspection during performance of the contract that will ensure the continued efficacy and efficiency of

safeguards and the discovery and countering of new threats and hazards. All DAS DCRB security related records will be made available as required for compliance with such inspections.

5.0 Security Contacts

5.1 District of Columbia Retirement System Key Personnel

Address District of Columbia Retirement System
900 7th Street, NW, Second Floor
Washington, DC 20001

Peter Dewar (202) 343-3215
Director Information Technology peter.dewar@dc.gov

Michaela Burnett (202) 343-3239
Applications Development Manager Michaela.burnett@dc.gov

5.2 DAS Key Personnel

Mailing Address Document Access Systems
703 Westchester Drive
Suite 105
High Point, NC 27262

Matt Weis (336) 882-8252
Vice President mweis@documentaccess.net

Fred Heilbronner (772) 341-6646
Solution Architect fheilbronner@documentaccess.net

Michael Wiese 678-451-5626
Project Manager mwiese@documentaccess.net
Information Security Manager

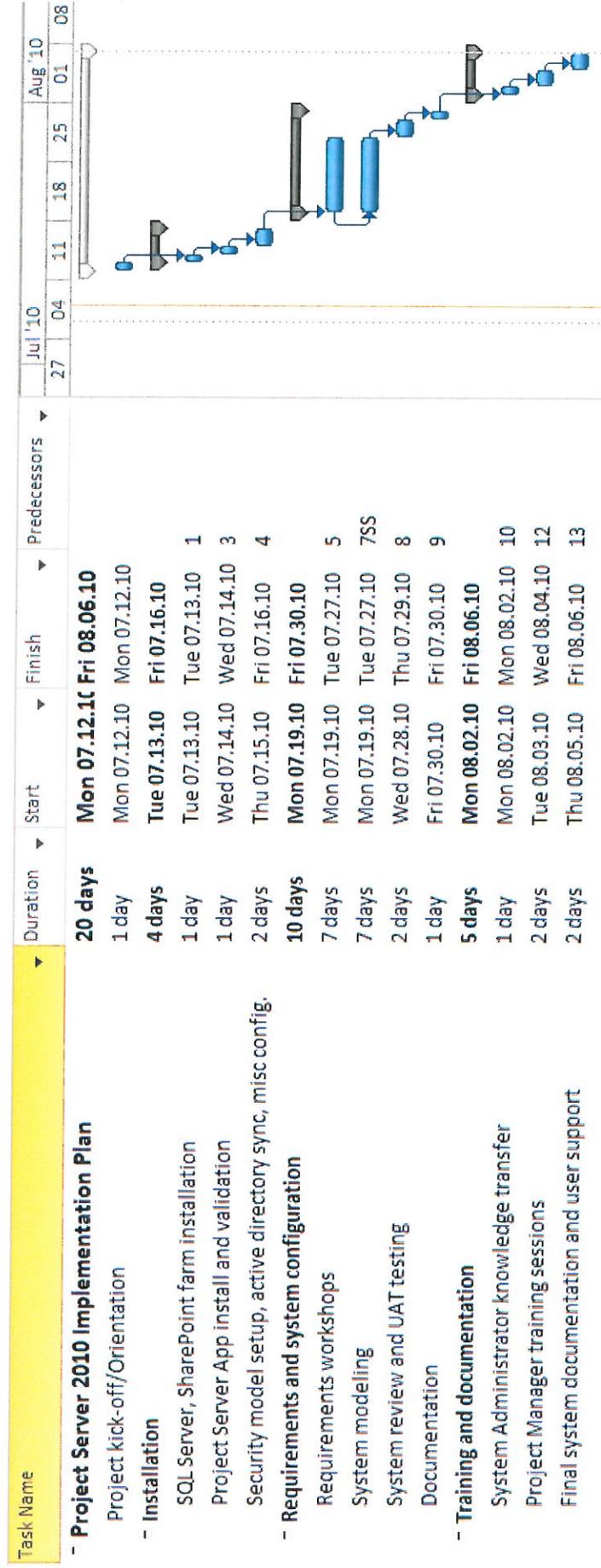
DCRB/PROJILITY
KICKOFF AGENDA AND SCHEDULE



Project Kickoff Agenda

- Project Team
- Project Objectives
- Project Scope
- Project Management
- High-level Project Timeline
- What do we need from DC RB?
- Project Deliverables
- Key Success Factors
- Project Logistics

Draft Project Schedule



DCRB EPM 2010 SOW SCOPE

DCRB has a desire to plan, implement and train key personnel on the Microsoft Project Server 2010 (EPM) application. Requirements have emerged to setup a base application environment, perform configuration activities, and provide end-user training and mentoring for IT staff. The application will be used to support project tracking and reporting, and act as an automation mechanism for capturing, selecting and managing projects across the IT portfolio.

DCRB has requested **PROJILITY** provide technical and business consulting services in support of this project.

To meet this requirement, **PROJILITY** will provide a full-time EPM consultant, for a period of four (4) consecutive business weeks onsite, to begin work on an agreed-upon date.

SCOPE OF WORK & ASSUMPTIONS

1. For a period of four (4) consecutive business weeks, comprised of twenty (20) work days, **PROJILITY** will provide a full-time, on-site EPM Consultant for DC RB. The **PROJILITY** resource will work a forty (40) hour work week during this engagement.
2. All services will be provided on-site at the DC RB offices in Washington, DC. DC RB will provide the necessary working facilities, including workstation, network, and phone access, needed to successfully meet responsibilities within this project.
3. Tasks to be performed during this engagement are listed below, as time allows. During the first day of work onsite, **PROJILITY's** EPM Consultant will work with the DC RB Project Manager to prioritize and allocate work to these tasks, based upon the specific needs of the DC RB organization:
 - Meet with key DC RB system and business stakeholders to review and assess current business needs for EPM
 - Meet with key DC RB IT staff to understand the current technical environment and develop a system architecture for EPM 2010
 - Assess DC RB needs with respect to Project Server 2010, including:
 - Roles and responsibilities
 - Reporting needs and system capabilities
 - Time tracking
 - Current DC RB project schedule creation processes
 - Planning and management of non-project resources and time
 - Desired project proposal and selection processes
 - Resource types within Project Server, including generic, named, and team resources, as well as resource calendar functionality
 - Current system and network architecture
 - Current and desired integration with Active Directory and email environments
 - Reporting
 - Perform installation and validation of a single Production environment of Project Server 2010
 - Perform system configuration activities based upon understanding of requirements captured
 - Delivery of hands-on training sessions for Project managers and Application/System Administrators

- Creation a roadmap document for future implementation, configuration, training and reporting recommendations for items NOT addressed during this initial engagement, as appropriate

DELIVERABLES

Work products delivered during this engagement will include:

- A Detailed project implementation plan
- A working Project Server/ SharePoint Server 2010 environment with secure remote access, integrated to DCRB's Active Directory.
- A working Portfolio Server environment
- DCRB's projects implemented into the Portfolio and ProjectServer parts of the system
 - Defined Benefit Pension System RFP
 - Data Reclamation Project
 - Business Process Reengineering
 - Enterprise IT Planning Project
 - Website Project
 - DCRB Image Project
- Project Server 2010 Installation Checklist
- Weekly status report
- Weekly status meeting attendance
- Findings and Recommendations document

PROJILITY
PROJECT STATUS REPORT
07.26.2010

Project Status Report

07/26/2010

Project Name DC Retirement Board
Reporting Period 7/18/2010 – 7/24/2010

General Project Status

Green – Project Finish date is projected to be 08/06/10.

Critical needs

- Tightening up configuration requirements and implementing in order to stabilize the system for training next week is critical.

Accomplishments for this period

- System Review and Requirements workshop conducted around basics system functionality, demand management, and SharePoint collaboration features conducted.
- Configuration requirements gathered in workshops implemented in system
- Standard project templates discussed and published to server for PM availability

Upcoming Activities and Milestones

- SharePoint 2010 and Project Server 2010 reinstalled on production servers
- SharePoint Project Site template discussed, constructed and implemented
- Final value lists for custom fields and misc configuration provided and implemented
- Basic enterprise reports created in preparation for executive user training

Issues

No issues at this time.

Risks

No risks identified at this time.

Project Schedule

Task Name	Duration	Start	Finish	% Complete
<input checked="" type="checkbox"/> Project Server 2010 Implementation	24 days	Tue 7/6/10	Fri 8/6/10	51%
Project kick-off/Orientation	1 day	Mon 7/12/10	Mon 7/12/10	100%
<input checked="" type="checkbox"/> Installation	4 days	Tue 7/13/10	Fri 7/16/10	100%
<input checked="" type="checkbox"/> Implementation - Week 1	5 days	Mon 7/19/10	Fri 7/23/10	100%
<input checked="" type="checkbox"/> Implementation - Week 2	19 days	Tue 7/6/10	Fri 7/30/10	0%
Status Meeting	1 hr	Mon 7/26/10	Mon 7/26/10	0%
Porfolio Analysis feature review	2 hrs	Mon 7/26/10	Mon 7/26/10	0%
Configuration	4 hrs	Mon 7/26/10	Mon 7/26/10	0%
SLL certificate, server rename and DNS alias status/review	1 hr	Mon 7/26/10	Mon 7/26/10	0%
Configuration	6 hrs	Tue 7/6/10	Tue 7/6/10	0%
SharePoint template construction	2 hrs	Tue 7/27/10	Tue 7/27/10	0%
Report Development	2 days	Wed 7/28/10	Thu 7/29/10	0%
Training Prep	1 day	Fri 7/30/10	Fri 7/30/10	0%
<input checked="" type="checkbox"/> Training and documentation	5 days	Mon 8/2/10	Fri 8/6/10	0%
Status Meeting	0.5 hrs	Mon 8/2/10	Mon 8/2/10	0%
System Administrator knowledge transfer	4 hrs	Mon 8/2/10	Mon 8/2/10	0%
Project Manager training sessions	2 days	Tue 8/3/10	Wed 8/4/10	0%
Final documentation (config tables, roadmap), admin support	2 days	Thu 8/5/10	Fri 8/6/10	0%

Action Items/Miscellaneous Items:

#	Action Item Description	Assigned to	Date Assigned	Date Needed by	<u>Completed?</u>
	Custom data choices for project fields, resource fields and administrative time categories needed	DCRB PMO	07/22/19	07/28/10	N
	Custom requirements for SharePoint workspace needed	DCRB PMO	07/16/10	07/28/10	N
	Server DNS alias requested from DCRB.	DCRB IT Support	07/14/10	07/30/10	N

PROJILITY
PROJECT STATUS REPORT
08.02.2010

Project Status Report

08/02/2010

Project Name DC Retirement Board
Reporting Period 7/26/2010 – 7/30/2010

General Project Status

Green – Project Finish date is projected to be 08/06/10.

Critical needs

- No critical needs at this time.

Accomplishments for this period

- System Review and Requirements workshop conducted around SharePoint project site template. Template put in production.
- Custom field and lookup table requirements finalized and implemented.
- Project Center and Project detail reports tightened up.
- Business Intelligence site configured for executive introduction.

Upcoming Activities and Milestones

- Project Manager and Administrator training sessions to be conducted.
- Executive reporting demo and question/answer session to be conducted.
- Configuration clean up and support issues resolved.
- Remaining documentation and close-out meeting to be conducted.

Issues

No issues at this time.

Risks

No risks identified at this time.

Project Schedule

Task Name	Duration	Start	Finish	% Complete
Project Server 2010 Implementation	24 days?	Tue 7/6/10	Fri 8/6/10	84%
Project kick-off/Orientation	1 day	Mon 7/12/10	Mon 7/12/10	100%
Installation	4 days	Tue 7/13/10	Fri 7/16/10	100%
Implementation - Week 1	5 days	Mon 7/19/10	Fri 7/23/10	100%
Implementation - Week 2	19 days	Tue 7/6/10	Fri 7/30/10	100%
Training and documentation	5 days?	Mon 8/2/10	Fri 8/6/10	0%
Status Meeting	0.5 hrs	Mon 8/2/10	Mon 8/2/10	0%
Project Manager training	2 hrs	Tue 8/3/10	Tue 8/3/10	0%
Admin training	1 hr	Tue 8/3/10	Tue 8/3/10	0%
Admin training	2 hrs	Wed 8/4/10	Wed 8/4/10	0%
Executive reporting overview/training	1 hr	Wed 8/4/10	Wed 8/4/10	0%
Final documentation (config tables, roadmap), admin support	1 day	Thu 8/5/10	Thu 8/5/10	0%
Project closeout/support issues	1 day?	Fri 8/6/10	Fri 8/6/10	0%

Action Items/Miscellaneous Items:

#	Action Item Description	Assigned to	Date Assigned	Date Needed by	Completed?
	SQL Backup routine and agents need to be reassigned to production servers, and away from test system	DCRB IT Support	07/16/10	ASAP	N
	Server DNS alias requested from DCRB.	DCRB IT Support	07/14/10	ASAP	N

PROJILITY, INC. CONTRACT

PROFESSIONAL SERVICES AGREEMENT
BETWEEN
THE DISTRICT OF COLUMBIA RETIREMENT BOARD
AND
PROJILITY, INC.

This Agreement is between the District of Columbia Retirement Board, hereinafter referred to as DCRB, and Projility, Inc., located at 8300 Greensboro Drive, Suite 800, McLean, VA 22102, hereinafter referred to as ("Projility").

WHEREAS, DCRB has requested to implement a project management system to track and monitor project deliverables, cost, contractor performance, tracking and reporting, and other relevant project and program management requirements as well as provide intranet capabilities through SharePoint technology;

WHEREAS, DCRB has identified the tool needed to meet the requirement as MicroSoft Project Server 2010. DCRB has a desire to plan, implement and train key personnel on the Microsoft Project Server 2010 (EPM) application that can achieve the agency objectives. Requirements have emerged to setup a base application environment, perform configuration activities, and provide end-user training and mentoring for IT staff. The application will be used to act as an automation mechanism for capturing, selecting and managing projects across the agency portfolio;

WHEREAS, DCRB has identified Projility as a company that has the experience and expertise in EPM implementation and configurations and is an authorized MicroSoft partner;

NOW, THEREFORE, the parties hereto, for the consideration hereinafter set forth, mutually agree as follows:

ARTICLE I. SCOPE OF WORK:

Section 1. Projility shall provide an EPM Consultant to assist DCRB in assessing its need with respect to MicroSoft Project Server 2010 and to create a MicroSoft Project Server 2010 production environment.

Tasks to be performed include:

- A. Identifying roles and responsibilities
- B. Identifying reporting needs and system capabilities
- C. Time tracking
- D. Creation of current DC RB project schedules and processes
- E. Planning and management of non-project resources and time
- F. Create and discuss with the Information Technology Specialist or his

- designee the desired project proposal and selection processes
- G. Developing resource types within Project Server, including generic, named, and team resources, as well as resource calendar functionality
 - H. Evaluate the current system and network architecture
 - I. Evaluate the current and desired integration with Active Directory and email environments
 - J. Provide reporting (written and oral)

Section 2. DCRB will provide the necessary working facilities, including workstation, network, and phone access, needed to successfully meet responsibilities within this project.

ARTICLE II. GENERAL REQUIREMENTS:

Section 1. Projility shall provide a project server 2010 installation checklist to the Information Technology Specialist or his designee.

Section 2. Projility shall meet with key DCRB's IT staff and to assess the technical environment and develop a written system architecture for EPM 2010.

Section 3. Projility shall create and provide a roadmap document for future implementation, configuration, training and reporting recommendations for items not addressed during this agreement, as appropriate, to the Information Technology Specialist or his designee.

Section 4. Projility shall provide a full-time, on-site EPM Consultant for DCRB. The EPM Consultant will be on-site at the DCRB office for a period of four (4) consecutive business weeks, comprised of twenty (20) work days. The Projility resource will work forty (40) hour each work week during the term of this agreement.

Section 5. Projility shall prepare and submit a written weekly status reports to the Information Technology Specialist or his designee.

Section 6. Projility shall participate in weekly onsite status meeting with the Information Technology Specialist to track all deliverables, provide status updates, etc.

Section 7. Projility shall perform installation and validation of a single production environment of project server 2010, perform systems configuration activities based upon understanding of requirements captured and delivery of hands-on training sessions for DCRB project managers and application/system administrators at no additional cost to DCRB.

Section 8. Projility shall provide a findings and recommendations document to the Information Technology Specialist or his designee.

Section 9. Projility shall provide a written detailed project implementation schedule.

Section 10. Projility shall provide a working Project Server/ SharePoint Server 2010 environment with secure access, integrated to DCRB's Active Directory.

Section 11. Projility shall provide a working Project Server 2010 environment. DCRB's projects listed below will be loaded into the Project Server 2010 environment

- A. Defined Benefit Pension System RFP
- B. Data Reclamation Project
- C. Business Process Reengineering
- D. Enterprise IT Planning Project
- E. Website Project
- F. DCRB Image Project

ARTICLE III. TERM OF AGREEMENT:

The term of this Agreement shall be for a period of four business weeks starting on an agreed-upon date after which the Agreement is last executed by DCRB and Projility. This Agreement may be terminated by DCRB in whole or in part for cause.

If DCRB proposes terminating the contract for cause, DCRB will first give ten (10) days prior written notice to Projility stating the reason for termination, and providing Projility an opportunity to cure the issues leading to termination.

Projility shall not be entitled to receive payment for labor or expenses incurred prior to termination unless accepted by DCRB.

This Agreement may be terminated in whole or in part by DCRB for the convenience of the Board at any time by giving Projility written notice. In such event:

- A. Projility shall immediately cease performing the terminated work unless directed otherwise.
- B. Projility shall be reimbursed for agreed upon fees and expenses incurred in preparing to perform the terminated work.
- C. Projility shall not be compensated for anticipated future profit for the terminated work.

ARTICLE V. COMPENSATION AND EXPENSES:

Section 1. Compensation under this Agreement shall not exceed **twenty-thousand eight hundred and twenty dollars and zero cents (\$20,820.00)**. Consulting services will be provided and costs covered based upon a combination of Microsoft Software Assurance Voucher funds covering ½ of the total project cost (\$20,000), plus DCRB funds to cover the second half of required funding (\$20,000). Training materials will also be provided at a cost of (\$820).

Payment terms will be Net 30 days. Invoices will be provided to DCRB on the first day following the month during which work has been performed, based upon actual hours worked. The total amount due to Projility from DCRB of \$20,820.00 will be invoiced as work is performed during the first half of the project. Software Assurance voucher funds will be utilized to cover work during the second half of the project.

Additional work deemed out of scope or beyond budget will require execution of a Change Order between DCRB and Projility outlining the impact on scope, cost, and deliverables.

ARTICLE VI. GENERAL PROVISION:

Section 1. Modification of Agreement. Any modification of this Agreement or additional obligation assumed by either party in connection with this Agreement shall be binding only if in writing and signed by Projility and DCRB's Chief Contracting Officer.

Section 2. Severability. This Agreement is severable. If any provision or term hereof is determined, for any reason, to be illegal or otherwise unenforceable, such determination shall not affect the validity of the remaining provisions and terms hereof. The provision or term determined to be illegal or unenforceable shall be amended to conform to applicable law and the intent of the Parties.

Section 3. Maintenance of Books and Records. Projility shall maintain all books and records related to the tasks and duties related to this Agreement on file at DCRB.

Section 4. Reports. All reports and documents produced in the performance of this Agreement shall be the sole property of DCRB. Projility shall make no distribution of work specifically produced for DCRB under this Agreement to others without the express written consent of DCRB.

Section 5. Assignments. Projility shall not subcontract any of the services of to be performed under this Agreement without the prior written consent of the contracting officer.

Section 6. Indemnification. Projility hereby agrees to hold harmless DCRB, its members, officers, employees, agents and representatives and the District of Columbia Government, and to indemnify and exonerate same against and in respect of any and all claims, demands, damages, actions, costs, charges, losses, liabilities, and deficiencies, including legal fees and expenses, resulting from, arising out of, or in any way related to: (a) any untrue warranty or representation

or omission of Projility in this Agreement; and/or (b) Projility's willful misfeasance, bad faith, negligence, or reckless disregard of its obligations under the terms of this Agreement.

Section 7. Governing Laws. This Agreement shall be governed by and construed in accordance with the laws of the District of Columbia.

Section 8. Dispute Resolution.

- A. The parties waive the right to trial by jury in any judicial action, proceeding or counterclaim arising from this Agreement that is not resolved by mutual agreement.
- B. Any legal proceedings involving this Agreement shall be filed with a District of Columbia court with subject matter jurisdiction, and District of Columbia law shall apply.
- C. Pending final settlement of or a final decision from a court on an action or appeal of, a dispute or a claim asserted by Projility against DCRB, Projility shall proceed diligently with performance of the Agreement in accordance with its terms and conditions.
- D. Neither party will, directly or indirectly, assign or transfer any claim arising out of this engagement.
- E. The failure of either party to enforce any of the terms of this Agreement shall not be a waiver or relinquishment of any future requirements of this Agreement.
- F. The section headers in this Agreement are for information only and shall not be used to construe the meaning of any particular clause.
- G. Projility shall discharge its duties and responsibilities under this Agreement with the standard of care, skill, and diligence normally provided by a technical consulting firm in the performance of similar services under similar circumstances.
- H. The rights and remedies described in this Agreement are cumulative and are in addition to any other remedies available to DCRB in law or in equity, and the exercise of any one or more of such remedies shall not be construed as a waiver of any other right or remedy.
- I. Projility shall promptly notify DCRB of any change in the availability of the personnel proposed to perform services under this Agreement, and shall propose a replacement who will be subject to acceptance by the DCRB.
- J. Projility shall assist DCRB in asserting a claim of privilege in a legal proceeding or exemption under a request for documents pursuant to the District of Columbia Freedom of Information Act.
- K. Projility shall perform such work as is necessary to correct errors, defects, and omissions in the services provided under this Agreement without undue delays and without cost to DCRB.
- L. The Contracting Officer unilaterally may order Projility in writing to suspend, delay, or interrupt all or any part of work it is performing without cost for such period of time as he may deem appropriate for the convenience of the DCRB.

- M. All work shall be performed in accordance with DCRB's conflict of interest guidelines, which are set forth at Attachment A, and the conflict of interest provisions at 7 DCMR §1548 (2006), both of which are incorporated by reference into and as part of this Agreement.
- N. Additional specific terms may be negotiated between DCRB and Projility on an "as needed" basis.
- O. In the event DCRB awards a successor agreement to another vendor covering the same matters as those assigned to Projility, then Projility shall cooperate with DCRB to effect an orderly transition to the successor vendor.

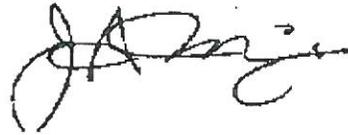
IN WITNESS WHEREOF, the parties have caused this Agreement to be executed as of the date last written below.

D.C. RETIREMENT BOARD:

PROJILITY, INC:



Eric O. Stanchfield
Executive Director &
Chief Contracting Officer



Jose A. Marroig
President

Dated: 6/24/10

Dated: 06/29/2010