Multnomah County
www.co.multnomah.or.us

Program # 72074 - IT - Information Security — Version 2/17/2006 s

Priority: Accountability
Lead Agency: County Management
Program Offer Type: Existing Operating
Program Contact: Becky Porter
Related Programs:
Program Characteristics: One-Time-Only Request, Backfill State/Federal/Grant

Executive Summary

Implementing, monitoring and maintaining information security is fundamental to supporting the Accountability initiative. Personally identifiable information such as health records, social security numbers, criminal history or credit card data all require the utmost care and protection. This program provides an independant, objective means to coordinate these efforts. Safeguarding both county and citizen information against threats and loss is a critical component in maintaining the public's trust and confidence. As county departments continue to extend their electronic connections into the community, new levels of security risk are created and must be monitored, managed and mitigated.

Program Description

The person hired via this program offer is responsible for making sure the County complies with all security mandates and requirements including HIPAA , Payment Card Industry (PCI) Security Requirements and Criminal Justice Information Systems (CJIS) regulations, as well as industry best practices. The program will coordinate consistent security policies across all county entities, including the DA and MCSO. In 2007 a comprehensive security review of all the County's Information Security practices, as required by HIPAA, is planned. Federal mandates require on-going compliance monitoring and reporting.

Program Justification

The county can receive significant fines if we are audited and found to be non-compliant in how we store, manage and secure information such as medical records. The County is working more with external partners which increases the amount of risk we need to manage including protecting our systems from virus and hacking activity. The County is working to enable electronic commerce transactions so that citizens can pay bills or transfer funds electronically. This means that personal credit or banking information travels through our systems and must be protected. Finally, the County is a public trust and, as such, is responsible for safeguarding the public's confidential information. The loss or theft of citizen's information can have significant financial, political and legal liability. A vivid illustration of why an information security program is essential is the recent theft of patient information from Providence Health Systems and the resulting investigation by the Oregon Attorney General's office. The County maintains similar data in a number of locations, so making sure it is secure and protected is extremely important.
IT research firm Gartner reports that "as a general rule, a security spending level of 3 percent to 6 percent of total IT budget should be the norm." This program offer represents a spending level of 0.7% of the total budget, far below average.

Performance Measures

Measure Type	Primary Measure	Previous Year Actual (FY04-05)	Current Year Purchased (FY05-06)	Current Year Estimate (FY05-06)	Next Year Offer (FY06-07)
Output	Information Security policies established or updated	15	0	0	10
Outcome	Security incidents reported	3	0	5	5
Output	Information security advice Requests Responded to	44	0	75	80
Output	Information security opinion rulings issued	18	0	50	50

Performance Measure - Description

1. Security Incidents are defined in County Administrative Rule and are tracked via manual and automated event logs on the network. 2. Information Security Policies are required by best practices and by several federal laws and rules 3. Information Security Issues arise regularly (historically around five or so per month). 4. Information Security Opinions are called for several times per month. These are also logged.

Legal/Contractual Obligation

Federally mandated Health Insurance Portability and Accountability Act of 1996 (HIPAA), Payment Card Industry (PCI) Security Requirements and Criminal Justice Information Systems (CJIS) Requirements.

Revenue/Expense Detail

	Proposed General Fund	Proposed Other Funds	Proposed General Fund	Proposed Other Funds
Program Expenses	2006	2006	2007	2007
Personnel	$0	$130,880	$0	$142,516
Contracts	$0	$0	$0	$120,000
Materials & Supplies	$0	$0	$0	$13,000
Internal Services	$0	$0	$282,294	$6,778
Subtotal: Direct Exps:	**$0**	**$130,880**	**$282,294**	**$282,294**
Administration	$0	$0	$0	$0
Program Support	$0	$0	$0	$0
Subtotal: Other Exps:	**$0**	**$0**	**$0**	**$0**
Total GF/non-GF:	**$0**	**$130,880**	**$282,294**	**$282,294**
Program Total:	**$130,880**		**$564,588**	
Program FTE	0.00	0.00	0.00	1.00
Program Revenues				
Fees, Permits & Charges	$0	$0	$0	$282,294
Other / Miscellaneous	$0	$130,880	$0	$0
Program Revenue for Admin	$0	$0	$0	$0
Total Revenue:	**$0**	**$130,880**	**$0**	**$282,294**

Explanation of Revenues

The first year cost of this program offer is $282,294 and will be funded with one time only General Fund. The cost of this program is not included in our FY05/06 Information Technology rates. It is currently funded with a combination of the Risk Management Fund and a portion of our BWC. Ongoing annual costs are predominantly related to FTE and are approximately $202,000 plus increases for COLA and Merit raises. These ongoing costs will be factored into the FY 2008 IT rates.

Significant Program Changes

Last year this program was: #71065, HIPAA Security Rule Compliance
This program was originally funded using BWC and risk management funds and is required to sustain HIPAA compliance. Failure to fund this program using new revenue and create a permanant security position will require IT to reassign assets from other program areas in order to maintain an acceptable level of information security throughout the County.