

Internal Audit Report on Personal Information Protection – General Services

County of Henrico



*Proud of our progress;
Excited about our future*

Internal Audit Report #238
August 9, 2013

HENRICO COUNTY INTERNAL AUDIT
<http://www.co.henrico.va.us/audit>
4301 EAST PARHAM ROAD
P.O. BOX 90775, HENRICO, VIRGINIA 23273-0775

Internal Audit Report on Personal Information Protection- General Services



Report #238
August 9, 2013



Summary

- Scheduled Audit
- Conclusions on Audit Objectives:
 - Controls are sufficient, insufficient or need improvement as follows:
 - ▲ Compliance oversight related to laws, regulations, policies and procedures
 - ▲ Collection, storage, dissemination and disposal of personal information
- Exception Oriented
- 3 reportable Issues; 3 Other Observations
- Management Action Plans have been developed to address all risks identified

● Insufficient-Immediate Attention ▲ Improvement Needed ■ Sufficient



Contents

- Introduction and Background
- Scope, Internal Controls and Methodology
- Conclusions on Audit Objectives
- Issues and Management Action Plans
- Closing and Report Distribution



Henrico County Internal Audit

3



Introduction

- Auditor III Sharon Wade performed audit work
- Used professional auditing standards
- Examined controls & tested for selective compliance
- All exceptions given to Agency
- Reported control design issues & significant test exceptions only
- Work for same Government we audit



Henrico County Internal Audit

4



Background



Code of Virginia

Government Data Collection and Dissemination Practices Act:

2.2-3800.B. *The General Assembly finds that:*

1. *An individual's privacy is directly affected by the extensive collection, maintenance, use and dissemination of personal information;*
2. *The increasing use of computers and sophisticated information technology has greatly magnified the harm that can occur from these practices;*

Henrico County Internal Audit

5



Background

Code of Virginia 2.2-3801. Definitions:

"Personal information" means all information that (i) describes, locates or indexes anything about an individual including, but not limited to, his social security number, driver's license number, agency-issued identification number, student identification number, real or personal property holdings derived from tax returns, and his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, or (ii) affords a basis for inferring personal characteristics..."Personal information" shall not include routine information maintained for the purpose of internal office administration whose use could not be such as to affect adversely any data subject nor does the term include real estate assessment information.



Henrico County Internal Audit

6



Background

Code of Virginia 2.2-3801. Definitions:

“Agency” means any agency...or like governmental entity of the Commonwealth or of any unit of local government including counties...



Background

Code of Virginia 2.2-3803:

A. Any agency maintaining an information system that includes personal information shall:

- 1. Collect, maintain, use, and disseminate only that personal information permitted or required by law to be so collected, maintained, used, or disseminated, or necessary to accomplish a proper purpose of the agency;*





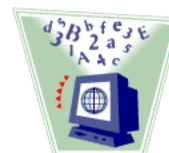
Background

Code of Virginia 2.2-3803. A. Cont'd

8. *Take affirmative action to establish rules of conduct and inform each person involved in the design, development, operation, or maintenance of the system, or the collection or use of any personal information contained therein, about all the requirements of this chapter...*



Background



Code of Virginia 2.2-3803. A. Cont'd

9. *Establish appropriate safeguards to secure the system from any reasonably foreseeable threat to its security;...*





Background

Personnel Rules and Regulations Section 14.8 Privacy of Information

...Each department is responsible for the safe-keeping and privacy of all personal information collected on employees and members of the public....

This section of Personnel Rules and Regulations was designed to comply with the Code of Virginia, Title 2.2-3803.A.8.



Background


Emerging Risk Regarding Confidential Information

During the course of this audit, research revealed that business identify theft is an emerging risk and guidance provided by BusinessIDTheft.org suggests that organizations should begin to treat Federal Identification Numbers (FIN's) associated with businesses in a manner similar to SSN's.

According to this website, identified misuses of FIN's has included impersonating a business: by using business' information to:

- *establish credit card accounts through which transactions are processed to:*
 - *benefit themselves or*
 - *provide a service to other criminals*
- *commit tax fraud or tax refund schemes by:*
 - *creating bogus W-2's*
 - *can then pretend to be the employee and file fraudulent tax returns resulting in tax refunds*
- *create bogus job offers which are used to collect personal information resulting in identity theft*










Background

General Services Organization:

- Facilities Management Division
 - Capital Projects
 - Energy Management
 - Buildings and Grounds
 - Custodial Services
 - Security Services
 - Food Services
- Support Services Division
 - Purchasing**
 - Records Management
 - Technology Support
 - Central Automotive Maintenance (CAM)
- Risk Management Division**
- Financial Division
- Administration






****Effective July 13, 2013, the Division of General Services was reorganized.**
 > Purchasing was moved to Finance
 > Risk Management was moved to Human Resources

Henrico County Internal Audit

13



Background

Personal/Confidential Information Collected:

Purchasing:


- SSN's/FIN's on Bid Proposals
- SSN's/FIN's on Supplier Add/Update Forms and W-9 Forms


Risk Management:

- SSN's & Dates of Birth on claim & Worker's Compensation forms
- Driver's License numbers and Dates of Birth on forms/reports related to DMV checks on individuals who operate County vehicles
- Claims processing system updated with bi-weekly downloads of personal data on all County employees from the HR system

Security Services:


- SSN's and Dates of Birth on Incident Reports






Henrico County Internal Audit

14



Background


Personal/Confidential Information Collected: 

Energy Management:

- SSN's on Davis-Bacon payrolls associated with one federal grant they received related to ARRA funds

Capital Projects:


- FIN's on Bid Proposals and American Institute of Architects (AIA) documentation


Buildings and Grounds: 

- SSN's/FIN's on Bid Proposals and AIA documentation

Food Services:

- Bank account numbers on checks received in the cafeteria each day (approximately 7 per management).

Henrico County Internal Audit  15



Scope



Includes:

- Purchasing
- Capital Projects
- Risk Management
- Energy Management
- Security Services
- Buildings and Grounds
- Food Services

And their related information systems that collect and store personal information

Excludes:

- All other Divisions of General Services including Health Insurance Administration (transferred to Finance effective 2/9/13) as it was determined that all claims reporting received by this area is “de-personalized”;
- All other information systems

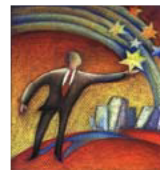
Henrico County Internal Audit   16



Internal Controls

Objectives

- Reliability and integrity of information
- Compliance with policies, procedures, laws and regulations
- Safeguarding of assets
- Effectiveness and efficiency of operations



Henrico County Internal Audit

17



Internal Controls


General Limitations of any Controls

- Errors and irregularities may go undetected
- Inherent limitations in any control structure
- Limitations include resource constraints, legislative restrictions, etc.
- Projection to future subject to risk of change in effectiveness
- Compliance may deteriorate




Henrico County Internal Audit

18




Audit Methodology

- Evaluated design of internal control system including certain relevant application controls using walk-throughs and/or questionnaires
- Tested selected system-related access controls



Henrico County Internal Audit 19




Conclusions on Audit Objectives

- ▲ **Objective 1** – Determine the effectiveness of compliance oversight related to laws, regulations, policies and procedures. *(Issues 1, 3 & 4)*
- ▲ **Objective 2** – Determine that controls over the collection of personal information are operating effectively. *(Issues 1, 2 & 3)*
- ▲ **Objective 3** – Determine that controls over the storage of personal information are operating effectively. *(Issues 1, 2 & 4)*
- ▲ **Objective 4** – Determine that controls over the dissemination of personal information are operating effectively. *(Issues 1, 2 & 3)*
- ▲ **Objective 5** – Determine that controls over the disposal of personal information are operating effectively. *(Issues 1, 2 & 4)*

● Insufficient-Immediate Attention ▲ Improvement Needed ■ Sufficient


Henrico County Internal Audit 20



Issues

General Services/Finance/Human Resources:

1. Enhance Controls over Personal Information
 - Risk Management
 - Purchasing
 - Security Services
 - Facilities Management
 - Agency-wide
2. Establish a Process to Protect Business Confidential Information



Information Technology:

3. Raise Awareness of Email Security

Other Observations:


4. Secure Other Sensitive Information - Security Services
5. Test System Upgrades Prior to Implementation - Risk Management
6. Implement System/Cash Handling Controls - Food Services

Henrico County Internal Audit 21

Issue 1


General Services/Finance/HR:

Enhance Controls over Personal Information



control

22




Issue 1

Criteria

- Jobs assigned to temporary employees are to be appropriate for non-employees considering limitations on background checks and requirements for confidentiality;
- Code of Virginia [Government Data Collection and Dissemination Practices Act]:
 - Title 2.2-3800.C.6: "There shall be a prescribed procedure for an individual to learn the purpose for which information has been recorded and particulars about its use and dissemination."
 - Title 2.2-3800 C.8: "Any agency holding personal information shall assure its reliability and take precautions to prevent its misuse."
 - Title 2.2-3803 A.1, "Any agency maintaining an information system that includes personal information shall: Collect, maintain, use, and disseminate only that personal information permitted or required by law to be so collected, maintained, used, or disseminated, or necessary to accomplish a proper purpose of the agency..."
 - Title 2.2-3803.A.9: "Establish appropriate safeguards to secure the system from any reasonably foreseeable threat to its security;"
- Virginia Administrative Code Chapter 120 - Regulations Governing the Destruction of Public Records Containing Social Security Numbers (17VAC15-120)
- As a related best business practice, restrictions should be placed on the number of individuals allowed to collect personal information in order to limit access to this data.

Henrico County Internal Audit 23




Issue 1


Condition

Risk Management:

1. A temporary employee working in Risk Management had access to confidential information given her read-only access to their claims system and her filing duties. This system access allowed her to view the entire SSN field; however, during the audit, this access was changed so she can no longer view this information. No paperwork outlining confidentiality expectations and consequences was reviewed with and signed by this individual. Furthermore, the contract with the company providing the temporary employees does not include a confidentiality clause. Finally, Purchasing shares this position with Risk Management.
2. Forms used to collect information for claims processing and DMV records checks do not contain a notice that completely describes the purpose and use of the personal information collected and specifics about its dissemination. Furthermore, the website lacks instructions on the secure transmission of forms containing personal information to this Division.



Henrico County Internal Audit 24




Issue 1

Condition

Risk Management:

3. We noted the following about the claims processing system which contains personal information on every County employee that is downloaded bi-weekly from Oracle:
 - a. the password change function had not been turned on; however, during the audit, this security setting was activated.
 - b. informal permission access reviews are performed; however, they are not documented.
4. At the start of the audit, claim files containing personal information were not always locked up at night. One compensating control is that the office suite is locked after the cleaning crew leaves.
5. In the recent past, after a staff member retired, personal information was downloaded to a thumb drive to make access easier for the individual assuming the duties. The Risk Manager stated that the thumb drive was secured in a locking cabinet, however, during the audit, it was destroyed after the information was moved to a secured network folder.
6. The user name and password used to access a generic Risk Management mailbox setup to receive claim information is published in the Division's work practices.
7. Permissions on network folders used to store claim-related files are not reviewed periodically.

Henrico County Internal Audit 25





Issue 1


Cause

Risk Management:

1. Temporary employees have been utilized in several different roles to support claims processing. These different roles require different accesses; however, in the past, temps have all been granted the same access.
2. Information concerning this chapter of the Code of Virginia and the overall security of personal information has not been communicated to all agencies that collect personal information as no position within the County has been assigned this responsibility.
3. Relatively small number of users, therefore, formalized system controls were not put in place
4. The password change function had not been activated since implementing the web-based version of the claims processing software.
5. Space constraints and reliance on the locked door to the office suite
6. The Division's work practices are distributed to the claims staff who have access to the information retrieved from the generic mailbox or who would be assigned to administer the claims.
7. Have not checked on network folder permissions as Risk Management employees rarely transfer within the County given their specialized skill set and no County-wide requirement to periodically check on folder permissions



Henrico County Internal Audit  26




Issue 1


Effect

Risk Management:

1. Without confidentiality safeguards, a temporary employee, about whom the County has limited background information, could misuse personal data.
2. Non-compliance with State regulations and the potential for the interception of physical or electronic documents containing personal information being transmitted to Risk Management which could lead to the misuse of this data
3. Potential for unauthorized access to personal information on ALL County employees if the system does not force password changes and permission access reviews are not formalized and documented
4. Potential for unauthorized access to the personal information in unsecured working claim files, on a thumb drive, or in network folders. There is also the potential for unauthorized access to the risk management generic email box if the password is not kept confidential.



Henrico County Internal Audit 27




Issue 1


Recommendation

Risk Management:

- 1a. The Director of Human Resources should ensure that County policies are created which address the consideration of appropriate duties for temporary employees.
- 1b. The Purchasing Manager should ensure that confidentiality clauses are included in all contracts with companies which provide temporary employees. If state contracts are used which the County will not be able to alter, then, at a minimum, appropriate training on the proper handling of confidential information should be given and individual confidentiality agreements signed and maintained.
- 1c. The Risk Manager should ensure that temporary employees handling personal information review and acknowledge County confidentiality policies.
2. The Risk Manager should ensure that all forms are updated with a notice that briefly explains the purpose, use and dissemination of all personal information collected. This notice should also include an overall statement explaining that information will be kept confidential by the County to the extent permitted by law. This notice should also be posted on the Risk Management forms section on the Intranet which should also be updated with instructions on the secure transmission of these forms.



Henrico County Internal Audit 28





Issue 1

Recommendation


Risk Management:

3. The Risk Manager should document permission access reviews of the claims processing system semi-annually.
4. The Risk Manager should periodically perform desk audits in the evening to ensure all working claim files are locked up.
5. The Risk Manager should ensure that personal information downloaded on thumb drives is encrypted or password-protected or, to best protect confidential data, a policy should be adopted to prohibit the downloading of this information to these portable drives.
6. The user name and password to the generic Risk Management email box should be deleted from the Division's work practices.
7. The Risk Manager should periodically review permissions to network folders where claim-related files are stored to ensure the access is appropriate.

Henrico County Internal Audit

29




Issue 1

Management Action Plan

#	Management Action Plan	Completed By	Date
1-RM-1a	Personnel Rules and Regs Section 14.8 will be updated to include policy regarding access to personal information by temporary employees, volunteers, etc and appropriate confidentiality measures.	Director of Human Resources	9/30/13
1-RM-1b	Purchasing will include in temporary service type contracts language requiring contractors to secure "non-disclosure" agreements from all employees assigned to work within areas of the County where confidential information is retained.	Purchasing Manager	9/1/13
1-RM-1c	Temporary Employees will be requested to sign the "Temporary Employee Non-Disclosure Agreement" regarding personal information and confidentiality.	Risk Manager	8/1/13

Henrico County Internal Audit

30




Issue 1

Management Action Plan

#	Management Action Plan	Completed By	Date
1-RM-2	Forms will be revised to include a notice re: purpose, use and dissemination of collected information. A statement will be posted on the Risk Management intranet site.	Risk Manager	8/31/13
1-RM-3	██████████ permission access will be reviewed and documented semi-annually.	Risk Manager	9/30/13
1-RM-4	Random desks audits will be performed to ensure working claims files have been secured. A record of random audits will be maintained.	Risk Manager	8/15/13

Henrico County Internal Audit 31




Issue 1

Management Action Plan

#	Management Action Plan	Completed By	Date
1-RM-5	Thumb drives are currentl_ not bein_ used. A policy has been implemented prohibiting the downloading of any personal information to a thumb drive.	Risk Manager	8/5/13
1-RM-6	Division Work Practice document has been revised to delete the password for the generic mailbox. Work Practice document has been redistributed to personnel.	Risk Manager	8/31/13
1-RM-7	Network folder permissions will be reviewed semi-annually for appropriate access.	Risk Manager	8/31/13

Henrico County Internal Audit 32




Issue 1


Condition

Purchasing:

1. Since the Oracle upgrade in November 2012, forms to add or update suppliers in the system have been emailed to Purchasing. Once received, the forms are printed out for data entry and are then stored until month-end in a locked drawer with the key hidden in a relatively unsecured location.
2. Section 4.5g of the Purchasing Manual indicates hard drives of County computers should be removed before the system is declared surplus, transferred, traded-in or disposed of in some other manner but does not provide further instructions on what to do with the drives once removed.



Henrico County Internal Audit 33




Issue 1

Condition


Purchasing:

3. As we walked through the security controls in the various in-scope divisions of General Services, it was suggested that the completion of the Supplier Add/Update Forms be centralized within an agency to one position in order to restrict access to the personal information documented on these forms. When presented with this idea, the Purchasing Manager stated that this would be a viable enhancement to their process as this position would be knowledgeable and trained to quickly and efficiently supply information needed to set-up a vendor in Oracle.

Furthermore, the Purchasing Manager confirmed that these forms are to be completed by County Personnel only. Based on this process, it appears that a notice on the forms outlining the purpose, use and dissemination of the personal information requested is not required; however, Purchasing has not developed a mechanism (e.g. employee script, handout, etc.) to ensure employees collecting this information from suppliers consistently communicate the County's purpose, use and dissemination practices per the Code of Virginia.





Henrico County Internal Audit 34

**Issue 1**


Cause

Purchasing:

1. This is how the process evolved since the supplier forms are no longer taxed to Purchasing.
2. The agency technology support staff members should know what to do with the hard drives once removed.
- 3a. These forms have historically been completed by the employee tasked with vendor oversight or coordination.
- 3b. No one position or agency within the County has been tasked with the responsibility to ensure compliance with privacy regulations.




Henrico County Internal Audit 35

**Issue 1**

Effect


Purchasing:

- 1a. Collection of personal information in paper form could potentially result in the misuse of the data if not properly secured.
- 1b. Access to documents containing confidential information maintained in a locked drawer when the keys are stored in a relatively unsecured location could result in access to and misuse of this information.
2. Potential for the misuse of confidential information on removed hard drives if mishandled by untrained personnel
- 3a. Inefficient vendor set-up process when Purchasing is not initially supplied all required paperwork
- 3b. Too many individuals potentially having access to personal information if forms are not completed by a central person in each agency
- 3c. Non-compliance with the Code of Virginia concerning proper notice addressing the purpose, use and dissemination of personal information collected



Henrico County Internal Audit 36



Issue 1



Recommendation

Purchasing:


- 1a. In order to reduce the accumulation and storage of paper forms containing both personal and business confidential information, the Purchasing Manager should contact IT to see if they have an extra monitor for the Support Specialist's desk so that the forms can be pulled up on one screen and the data entry into Oracle can take place on the second screen, therefore, not requiring printing of the forms for data entry purposes.
- 1b. Keys to locked drawers containing confidential information should be maintained in a more secured location.
2. The Purchasing Manual should be updated with instructions on what to do with the hard drives once removed.
- 3a. The Director of Finance should request each agency head to designate one position to be assigned the responsibility of gathering all necessary information from vendors in order to complete the Supplier Add or Update Forms. This process should then be documented in the Purchasing Manual with the appropriate revisions made to the forms.



Henrico County Internal Audit

37


Issue 1



Recommendation


Purchasing:

- 3b. The Purchasing Manager should work with the County Attorney's Office to develop a mechanism to ensure County personnel collecting the information from suppliers and completing the New Supplier or New Election Official Add Request Forms are able to consistently communicate the County's purpose, use and dissemination practices (including under what authority personal information can be collected) as required per the Code of Virginia.



Henrico County Internal Audit

38




Issue 1

Management Action Plan

#	Management Action Plan	Completed By	Date
1-PUR-1a	Purchasing will install additional monitors on the desks of the employee's that will be responsible for data entry. This will eliminate the need for printing of documents.	Purchasing Manager	8/9/13
1-PUR-1b	Keys will be maintained in a more secure location.	Purchasing Manager	8/1/13

Henrico County Internal Audit 39




Issue 1

Management Action Plan

#	Management Action Plan	Completed By	Date
1-PUR-2	Purchasing Manual will be revised with expected issuance no later than Fall 2013. The guidelines for security of data contained on hard drives are provided by Information Technology. Information provided by IT will be included in the revised manual as follows under 4.5 g: <i>Therefore, all hard drives in County/School computers shall be removed from the chassis or cabinet by the department/school before the computer system is declared surplus, transferred, traded-in, or otherwise disposed of. All County departments should turn their hard drives over to Information Technology. Contact the IT Help Desk at 501-4357 for instructions. School's hard drives should be turned over to School Information Technology.</i>	Purchasing Manager	11/1/13

Henrico County Internal Audit 40




Issue 1

Management Action Plan

#	Management Action Plan	Completed By	Date
1-PUR-3a	Finance will develop guidance and issue to departments by use of Memorandum. The guidelines will encourage the Department to designate an individual(s) with responsibility for preparation and submission of Add/Update Forms. Purchasing Manual will be revised to address this audit issue. Forms will be updated as necessary.	Director of Finance; Purchasing Manager	12/31/13
1-PUR-3b	Applicable forms will be edited to contain the following information; <i>This information will be used to prepare year-end tax forms and to satisfy the requirement of Va. Code § 2.2-4354(2). The information will not be disseminated to third parties unless required by law.</i> In addition, the Purchasing Manual will include information in the appropriate section.	Purchasing Manager	9/1/13

Henrico County Internal Audit 41




Issue 1

Condition

Security Services:

- As of the start of the audit, personal information was collected on Security Services' Incident Report Forms as they contained fields for Social Security Number (SSN) and Date of Birth (DOB) which were not needed for their records. During the audit, the form was revised to delete the fields requesting date of birth and SSN. Additionally, in February 2013, Security officers were trained on the new process to not collect this personal information.
- Incident Reports which potentially contained personal information were emailed to the Building and Grounds Division of General Services upon their request in order to ensure that the proper paperwork documenting the incident was prepared for liability claim purposes.
- Permissions on an electronic folder containing completed Incident Reports sent to Risk Management include the Facilities Manager. Further review revealed that permissions to this folder were not updated based on the reorganization that took place after the last Director of General Services assumed the position in July 2011. (Under the former structure, Security Services reported to the Facilities Manager.)

Henrico County Internal Audit 42




Issue 1

Security Services:


Cause

1. This was the Incident Report Form that had always been used.
2. Incident Reports have always been shared in this manner.
3. Permissions to electronic folders containing personal information have not been reviewed periodically.


Effect



1. Potential for the misuse of confidential information collected and disseminated if that data is not properly secured and, as a result, falls into the wrong hands
2. Non-compliance with the Code of Virginia



Henrico County Internal Audit 43




Issue 1


Recommendation

Security Services:

1. Going forward, the Chief of Security Services should ensure that Incident Reports are only shared with those Divisions or agencies that need it to carry out their responsibilities or as required by law.
2. In conjunction with the agency-wide recommendation on slide 52, the Chief of Security Services should periodically review the permissions granted to any electronic folder containing personal information to ensure all access is appropriate. Documentation of this review should also be maintained.



Henrico County Internal Audit 44




Issue 1

Management Action Plan

#	Management Action Plan	Completed By	Date
1-SS-1	Will authorize distribution of any Incident report(s) being requested by any County Agency to ensure reason for distribution is necessary.	Chief of Security Services	7/31/13
1-SS-2	See response below 1-Agency-wide	Chief of Security Services	8/1/13

Henrico County Internal Audit 45




Issue 1


Condition

Facilities Management:

Discussion with , er personnel in the Facilities Mana_ement Division of General Services revealed that one employee has placed Supplier Add/Update forms which contain SSN or FIN data in an individual blue recycling bin after the information was sent to Purchasing.



Henrico County Internal Audit 46



Issue 1


Facilities Management:

Cause


No established procedures on how to properly dispose of this information

Effect

Potential for the misuse of confidential information included on documents that are not securely destroyed



Henrico County Internal Audit 47




Issue 1


Recommendation

Facilities Management:

The Supplier Add/Update forms should be updated with instructions to securely store or dispose of these documents given the sensitive data they contain. Furthermore, the Purchasing Manual should be updated with this same guidance.



Henrico County Internal Audit 48




Issue 1

Management Action Plan

#	Management Action Plan	Completed By	Date
1-FM	Purchasing will revise applicable forms and provide guidance to Departments as to proper handling of sensitive information related to supplier information. Refer to 1-PUR-3a.	Purchasing Manager	9/1/13

Henrico County Internal Audit 49

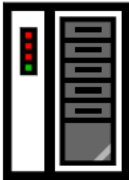


Issue 1


Condition

Agency-wide:

A review of system files revealed that three subfolders on one server used by General Services known to contain personal information were not secured even though they included some amount of confidential data. Once this issue was brought to management's attention, the folders were secured during the audit. There are 11 total servers assigned to the agency.



Henrico County Internal Audit 50



Issue 1

Agency-wide:


Cause

Oversight; did not realize that access to these subfolders had not been restricted

Effect

Unrestricted access to personal information stored on subfolders of servers could result in the potential misuse of this data.

Henrico County Internal Audit 51




Issue 1


Recommendation

Agency-wide:

... recommend that access to server folders that contain personal information be monitored periodically and restricted to only those users who have a business need for the information.



Henrico County Internal Audit 52



Issue 1

Management Action Plan


#	Management Action Plan	Completed By	Date
1-Agency-wide	General Services will utilize Sysinternals Software to generate reports that would show the permissions on each folder on a server. The software has been installed on the GS Technology Support Specialist computer. The program will run a bi-annual report and have each Division Director review the user permission within their section. Division Director's will notify the Technology unit within GS when there is a new hire or termination or change in shared folder permissions.	Director of General Services; Technology Support Specialist II	8/1/13

Henrico County Internal Audit 53


Issue 2

Finance:

Establish a Process to Protect Business Confidential Information




54




Issue 2

Criteria

Guidance on BusinessIDTheft.org, a website dedicated to business identity theft protection which was created by the National Association of Secretaries of State and the Identity Theft Protection Association, states, "Treat and protect your business EIN/TIN as you would your own Social Security number".




Henrico County Internal Audit 55




Issue 2

Condition

At the beginning of the audit, the Purchasing Manager asked if the Federal Identification Numbers (FIN's) assigned to businesses are considered confidential information. As a result, Internal Audit researched the issue and found that business identity theft is an emerging risk. Therefore, during the audit and in order to minimize the risk associated with the collection of this information, the Purchasing Manager established internal controls to only request supplier SSN's or FIN's when the contract is awarded and not when the initial bids/proposals are received. Procedures do not currently exist related to the protection of sensitive business information throughout its lifecycle at the County and, thus, no related employee education has taken place.




Henrico County Internal Audit 56




Issue 2

Cause

Business identity theft is an emerging risk; therefore, the protection of FIN's has not received the attention that has been focused on SSN's.




Henrico County Internal Audit 57




Issue 2

Effect

The potential for access to and misuse of business confidential information




Henrico County Internal Audit 58



Issue 2


Recommendation

We recommend that the Director of Finance work to establish a process to secure business confidential information (FIN's most importantly) throughout its lifecycle. This process should include steps to only collect and share business confidential information when needed to carryout job responsibilities.



Henrico County Internal Audit

59



Issue 2

Management Action Plan

#	Management Action Plan	Completed By	Date
2-Finance	In an effort to be proactive, the Department of Finance through Accounting and Purchasing will develop policies and procedures to ensure the safeguarding of this information in the future.	Director of Finance	12/31/13

Henrico County Internal Audit

60

Issue 3

Information Technology:
Raise Awareness of Email Security



61

Issue 3




Criteria

- Code of Virginia, Title 2.2-3803 A.5 which states, "Make no dissemination to another system without, (i) specific requirements for security and usage including limitations on access thereto, and (ii) receiving reasonable assurances that those requirements and limitations will be observed..."
- Code of Virginia, Title 2.2-3803 A.9 which states, "Establish appropriate safeguards to secure the system from any reasonably foreseeable threat to its security..."



Henrico County Internal Audit


62




Issue 3

Condition

Discussion with IT personnel and audit work revealed that the security of email communications sent or received via the internet cannot be guaranteed unless specific actions are taken to encrypt the contents. We noted that one Division worked with an outside vendor to obtain data via email that contained personal information and no proactive measures were taken to ensure its security (e.g. password protection of data or encryption of the transmissions).



Henrico County Internal Audit 63



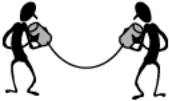
Issue 3

Condition


Internal email communications (defined as using the same Exchange server) are secured since the transport connection is encrypted. General Government, the Division of Police and the Department of Mental Health and Developmental Services all utilize the same Exchange server so email communications among these agencies are considered internal and, thus, secured.

However, Public Libraries and Schools each have their own Exchange servers; therefore, email communications between these entities and a General Government agency, the Police or MH/DS utilize the internet and are not necessarily secured.

During the audit, we noted that 39% of the emails related to supplier additions or updates received in the Purchasing Division in April 2013 were sent by Schools or Public Libraries and, thus, were not secured.




Henrico County Internal Audit 64




Issue 3

Cause

- Assumption that the email system is secure
- To date, there has not been any proactive on-going education for agencies on the relative insecure nature of emails and alternative mechanisms for securing such information.




Henrico County Internal Audit 65




Issue 3

Effect

Potential for email transmissions containing personal information that are sent from an external mail server to our mail server (or vice versa) to be intercepted over the internet with intentions to misuse the personal data content. Furthermore, there is the potential for emails to be picked up off of network equipment such as routers and switches; however, internet users typically trust the service providers (ISPs) to protect their network equipment.



Henrico County Internal Audit 66




Issue 3

Recommendation


We recommend the following:

1. In conjunction with the development of an on-line security awareness program for employees as recommended in Audit #174 Appropriate Computer Use, the Director of Information Technology should ensure that this program includes periodic communications which highlight these security considerations about email transmissions so every employee knows they should consider the content of the data in attachments or in the body of the email as well as the location of the recipient before it is sent. These communications should also provide information on free data encryption services if it is determined that personal information does, in fact, need to be sent via the internet.
2. The Director of Information Technology should ensure that the Computer and Other Information Systems Use Policy is updated to highlight and address secure transmission of personal information via email.

Henrico County Internal Audit



67



Issue 3

Management Action Plan

#	Management Action Plan	Completed By	Date
3-IT-1	IT is in the process of installing the Movelt software which will manage secure file transfers including encrypted email. Once installed there will be training sessions with the Henrico General Government TSSs on the use of the product. IT will also focus on certain agencies such as Mental Health, HR, Police and Social Services for instruction in the use of this new product.	IT Security Officer	11/1/13
3-IT-2	IT will conduct a review of current County Policies and modify them to include language addressing the secure transmission of personal information.	IT Security Officer	11/1/13

Henrico County Internal Audit

68



Other Observations

The following slides include additional observations noted during our audit which were considered less critical in reaching our conclusions on our audit objectives.



Henrico County Internal Audit

69



Issue 4


Secure Other Sensitive Information – Security Services

Discussion with management revealed the following:

1. Field notes taken to record information related to an incident in order to later prepare an Incident Report at a Security Services' site may not always be securely disposed of and there is no policy statement to guide proper disposal. In the past, these notes may have contained personal information such as SSN and date of birth. Since February 2013, personal information is no longer collected; however, the notes and subsequent Incident Reports could still document potentially sensitive occurrences such as assaults.
2. At the Eastern Government Center, there is a locked closet which can be used to secure completed Incident Reports; however, within this area, there is no secured filing cabinet. The Chief of Security Services stated that he would obtain a locking file cabinet from Surplus Property in order to secure these reports and any other items needed by officers to perform their duties within this closet area.

Henrico County Internal Audit

70




Issue 4


Recommendation:

We recommend the following:

1. The Chief of Security Services should update Standard Operating Procedures and institute training which addresses the proper destruction of field notes that could potentially contain documentation concerning sensitive incidents.
2. We concur with the Chief of Security Services' recommendation related to obtaining a locking file cabinet from Surplus Property to be placed in the secured closet at the Eastern Government Center in order to temporarily lock up reports until they are retrieved by Security personnel and placed in secure files in the Security Offices at the Government Center.



Henrico County Internal Audit
71




Issue 4

Management Action Plan

#	Management Action Plan	Completed By	Date
4-SS-1	Chief of Security will update Standard Operating Procedures to provide outline on the proper destruction of the use of field notes by Security Personnel and will be responsible for conducting initial training and periodic reviews to ensure compliance.	Chief of Security Services	9/1/13
4-SS-2	Security Services will position a Securable filing cabinet at the Eastern Government Center Security post to utilize to secure completed incident report(s) until they can be collected and returned to Security Services at Government Center for permanent filing in secured cabinet.	EGC Security Officers; Security Sergeants; Chief of Security Services	7/22/13

Henrico County Internal Audit
72




Issue 5

Test System Upgrades Prior to Implementation – Risk Management


We noted through discussion with management that upgrades to the claims processing system are not tested prior to being installed.

Recommendation:

System upgrades should be tested prior to installation and the testing results should be documented.



Henrico County Internal Audit
73



Issue 5

Management Action Plan

#	Management Action Plan	Completed By	Date
5-RM	Risk Manager will discuss with the Riskmaster vendor and IT support the feasibility of testing any future upgrade on a training database before final implementation of the upgrade.	Risk Manager	12/31/13

Henrico County Internal Audit
74



Issue 6

Implement System/Cash Handling Controls – Food Services

We noted the following during a walkthrough of the cafeteria closeout process:

1. The cashiering system password which the Food Services Manager uses to sign on and closeout the transaction day had not been changed since the system was implemented two and a half years ago. Furthermore, the user ID and password were posted on a clipboard in the Manager's locked office and were listed in the Employee Cafeteria Cash Handling Procedures for easy access by staff who serve as backups. During the audit, the Food Services Manager changed the password and indicated that it will be changed at least twice a year going forward. Management further agreed to take the user ID and password out of the Procedures Manual and to remove the _ostin_ from the cli_ board in the locked office.
2. The Food Services Manager stated that she had a 4 digit code to run reports on the registers in the cafeteria. Further discussions concerning the system password, however, prompted her to contact the vendor who helped her set-up individual manager codes for the registers. Apparently, the Food Services Manager had been sharing her code for the registers with those employees who back up her function.

Henrico County Internal Audit

75



Issue 6


Recommendation:

We concur with management's actions taken during the audit and recommend that the Employee Cafeteria Cash Handling Procedures be updated to reflect these changes.



Henrico County Internal Audit

76




Issue 6

Management Action Plan


#	Management Action Plan	Completed By	Date
6-Food Svcs.	User name and passwords issued to each person and will be changed twice per year. Policies and procedures will be updated to reflect these changes.	Food Services Manager	10/15/13

Henrico County Internal Audit 77




Closing

- Appreciate Agency's cooperation
- Follow up on open Action Plans will be performed as completion dates are reached




Henrico County Internal Audit 78



Report Distribution

Audit Committee (Mr. Glover, Mrs. O'Bannon, County Manager)	Board of Supervisors, Non-Committee Members
Deputy County Manager for Administration	Directors of General Services, Finance, Human Resources & Information Technology
Internal Audit Staff	

Henrico County Internal Audit 79



Audit Contact Information

Sharon Wade, Auditor III
Phone: 804-501-4210
E-Mail: wad01@co.henrico.va.us

Vaughan Crawley, Director of Internal Audit
Phone: 804-501-4292
E-Mail: cra85@co.henrico.va.us

Henrico County Internal Audit 80