Mecklenburg County
Department of Internal Audit

Business Support Services Agency
Computer and Equipment Disposal Audit Follow-Up
Report 1575

April 19, 2016

Internal Audit's Mission	To support key stakeholders in cultivating an environment of accountability, transparency and good governance.
Internal Audit Contacts	Joanne Prakapas, CPA/CFF, CIA, CFE, CRMA, Audit Director (980) 314-2889 or joanne.whitmore@mecklenburgcountync.gov Christopher Waddell, CIA, CRMA, Audit Manager (980) 314-2888 or christopher.waddell@mecklenburgcountync.gov
Staff Acknowledgements	Rick Kring, CISA, Auditor-In-Charge Deborah Caldwell, CIA, CISA, Information Technology Auditor
Obtaining Copies of Internal Audit Reports	This report can be found in electronic format at http://charmeck.org/mecklenburg/county/audit/reports/pages/default.aspx

MECKLENBURG COUNTY
Department of Internal Audit

To: Dena Diorio, County Manager

From: Joanne Prakapas, Director, Department of Internal Audit

Date: April 19, 2016

Subject: Business Support Services Agency Computer and Equipment Disposal Audit Follow-Up Report 1575

The Department of Internal Audit completed a follow-up audit on reported issues from the Business Support Services Agency Computer and Equipment Disposal Audit Report 1352 issued June 10, 2014. The objective of the follow-up audit was to determine with reasonable but not absolute assurance whether management took effective corrective action on the issues presented in the audit report.

Internal Audit staff interviewed key personnel, observed operations, reviewed written policies and procedures and other documents, and tested specific transactions where applicable. Internal Audit conducted this audit in conformance with The Institute of Internal Auditor's International Standards for the Professional Practice of Internal Auditing.

FOLLOW-UP SUMMARY

There were three recommendations in the Business Support Services Agency Computer and Equipment Disposal Audit Report 1352. The following table summarizes the results of the follow-up audits performed to date.

Recommendation Summary					
Fiscal Year	**Audit Report**	**Implemented**	**Open**	**Not Implemented**	**Withdrawn**
2015	1575	1	2		

Details regarding the most recent follow-up audit are noted in the attached **Follow-Up Results** matrix. Recommendations considered implemented will be excluded from further review. For those that remain open, Internal Audit will conduct a follow-up audit at a later date to verify they are fully implemented and working as intended.

The cooperation and assistance of the Information Technology staff are recognized and appreciated.

c: Deputy County Manager/Chief of Staff
Assistant County Managers
Deputy County Attorney
Senior County Attorney
Board of County Commissioners
Audit Review Committee
Chief Information Officer, Information Technology

Follow-Up Results
Business Support Services Agency Computer and Equipment Disposal Audit Report 1352

- **Implemented –** Audit issue has been adequately addressed by implementing the original or alternative corrective action plan **(I)**
- **Open –** Corrective action for audit issue initiated but not completed **(P)**; Implemented but not operating as intended **(IO)**; Not been addressed but management fully intends to address issue **(O)**
- **Not Implemented** – Audit issue not addressed and management has assumed the risk of not taking corrective action **(NI)**
- **Withdrawn** – Audit issue no longer exist due to operational changes **(W)**

				Implementation Status	
Risk Observation	**Recommendation**	**Management's Risk Mitigation Strategy**	**Original Implementation Date**	**Current Status**	**Comments**
1.1	Internal Audit recommends management develop formal, documented policies and procedures for computer and equipment disposal activities that reflect current and best practices, and train staff as necessary. The policies and procedures should include, at a minimum: • Staff roles and responsibilities for computer disposal activities • Computer pre-disposal physical security • Reconciliation between computer intake and destruction • Hard drive sanitation methodology and timing • Annual inventory requirements • Policy application, including exceptions • Periodic review and update of policies and procedures	Policies and procedures are presently being reviewed and amended to align computer and equipment disposal best practices with our business policies, processes and procedures. The aforementioned review and amendment process will be fully implemented by September 30, 2014. Benchmarked guidelines will be derived from NIST Special Publication-800-88.	09/2014	P	Management indicated the recommendation is partially implemented due to facility and leadership changes, which delayed completion.
2.1	Internal Audit recommends management reconcile computers slated for destruction against the vendor's settlement reports, which denotes computer hard drives that have been destroyed.	Reconciliation between disposal vendor and computer inventory list verifying decommissioning will occur quarterly and exceptions will be reported to information security within one business day. Information security will then work with all interested parties to remediate the discrepancy and provide a detailed report to BSSA-IT senior	06/2014	O	Management indicated the recommendation is open due to facility and leadership changes, which delayed implementation.

Follow-Up Results
Business Support Services Agency Computer and Equipment Disposal Audit Report 1352

- **Implemented –** Audit issue has been adequately addressed by implementing the original or alternative corrective action plan **(I)**
- **Open –** Corrective action for audit issue initiated but not completed **(P)**; Implemented but not operating as intended **(IO)**; Not been addressed but management fully intends to address issue **(O)**
- **Not Implemented** – Audit issue not addressed and management has assumed the risk of not taking corrective action **(NI)**
- **Withdrawn** – Audit issue no longer exist due to operational changes **(W)**

				Implementation Status	
Risk Observation	**Recommendation**	**Management's Risk Mitigation Strategy**	**Original Implementation Date**	**Current Status**	**Comments**
		leadership.			
3	Internal Audit recommends management implement procedures to sanitize hard drives in computers designated for destruction prior to vendor pick-up.	After a determination has been made to either reuse or destroy the device, the hard drive of that device will either be reused or destroyed. Any device slated for reuse will have the hard drive(s) sanitized in accordance with Department of Defense (DOD) standard 5220.22-M. Devices scheduled to be destroyed, will undergo hard drive(s) extraction. Computer information such as serial number, service tag number, hard drive identification numbers, and other information contained in the Certificate of Sanitization will be recorded in the destruction log. Drives set aside for destruction will then be physically destroyed via a hard drive destruction device. The desktop team will retain each hard drive for two weeks after its receipt from the employee. The data will serve as a back-up ensuring all migrated data has been transferred to the employee's new computer.	06/2014	I	