Mecklenburg County
Department of Internal Audit

Information Technology
Mobile Device Inventory Management Follow-Up Audit
Report 1914

May 14, 2020

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, CRMA, CFE, Audit Director (980) 314-2889 or joanne.prakapas@mecklenburgcountync.gov Christopher Waddell, CIA, CRMA, Audit Manager (980) 314-2888 or christopher.waddell@mecklenburgcountync.gov
Staff Acknowledgements	Deborah Caldwell, CIA, CISA, Auditor-in-Charge
Obtaining Copies of Internal Audit Reports	This report can be found in electronic format at https://www.mecknc.gov/audit/reports/pages/default.aspx?

MECKLENBURG COUNTY
Department of Internal Audit

To: Dena Diorio, County Manager
County Manager's Office

From: Joanne Prakapas, Director
Department of Internal Audit

Date: May 14, 2020

Subject: Information Technology Mobile Device Inventory Management Follow-Up Audit Report 1914

The Department of Internal Audit completed a follow-up audit on reported issues from the Information Technology Mobile Device Inventory Management Report 1662 issued December 18, 2018. The follow-up audit objective 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, 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 fifteen recommendations in the Information Technology Mobile Device Inventory Management Report 1662. The following table provides the original number of recommendations and summarizes the follow-up audit results performed to date.

Fiscal Year	Audit Report	Implemented	Open	Not Implemented[1]	Withdrawn	Total Carryforward
2018	1662[2]	N/A				15
2019	1914	4	11			11

[1] Management assuming risk for not taking corrective action
[2] Initial report

The attached **Follow-Up Results** matrix provides details for the most recent follow-up audit. Internal Audit will review any carryforward issues later to verify recommendations are fully implemented and working as intended.

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

c: Assistant County Managers
County Attorney
Senior County Attorney
Board of County Commissioners
Audit Review Committee
Chief Information Officer, Information Technology Services

Follow-Up Results
Information Technology Mobile Device Inventory Management Report 1662

- **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 ITS management develop and document formal policies and procedures for mobile device inventory management. Staff should be trained accordingly. The policies and procedures should be consistent with applicable County requirements, and include at a minimum: • Essential operating activities e.g., acquisition, purchase, storage, transfers, deployment, decommissioning, physical security, system access, x, segregation of duties, document retention, and management oversight • Staff training requirements • Staff roles and responsibilities • Periodic procedure reviews and updates • Internal and external communication requirements	• Develop a centralized IT asset management function responsible for lifecycle management, protection and controls of County software and technology equipment. • Update existing policies and procedures for mobile device inventory management • Update existing policies and procedures for mobile device utilization • Post new policies and procedures on Meckweb for employee access	10/2019	IO (2)	Internal Audit determined policies and procedures did not address some key operating activities, e.g., physical inventory, segregation of duties, document retention, and management oversight.
1.3	Internal Audit recommends ITS management, in collaboration with County departments, develop and document consistent and comprehensive policies and procedures for enterprise mobile device management and utilization.	• Develop a centralized IT asset management function responsible for lifecycle management, protection and controls of County software and technology equipment.	10/2019	P	Management indicated the recommendation is partially implemented. The ITS Asset Management team is working with Public Information to create MeckEDU training modules regarding the asset management lifecycle, monitoring, and inventory management.

Follow-Up Results
Information Technology Mobile Device Inventory Management Report 1662

- **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**
	The policies and procedures should be consistent with applicable County requirements, and leading best practices, such as: • ‘’ • Developing department guidance for the mobile device lifecycle, including usage monitoring and inventory management.	• Update existing policies and procedures for mobile device inventory management • Update existing policies and procedures for mobile device utilization • Post new policies and procedures on Meckweb for employee access			
2.1	Internal Audit recommends ITS management develop and maintain an inventory of all mobile devices. Moreover, ITS should implement processes and controls that utilize inventory and asset management best practices, such as: • Perpetual inventory listings for all mobile devices • Independent count, reconciliation, and verification • Physical inventory discrepancy follow-up • Segregation of duties	Build an IT Asset Management function within ITS responsible for enterprise technology asset management and capture a comprehensive inventory of mobile devices.	12/2019	P	Subsequent to the completion of audit fieldwork, management indicated the recommendation has been implemented and is pending Internal Audit's review.
3.1	Internal Audit recommends AFM and ITS management limit physical access to the central warehouse and mobile device storage locations to only authorized staff with a business need. Further, management should periodically review physical access	ITS management will limit access via badge authorization to specific staff. Additionally, ITS will store mobile device inventory in a locked storage room controlled by badge access to limited staff and review physical access controls at least annually with the understanding that	11/2018	I (3)	

Follow-Up Results
Information Technology Mobile Device Inventory Management Report 1662

- **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**
	permissions. Last, management should retain documentation of their review.	terminated employees are already immediately removed from the network including access control databases.			
4.1	Internal Audit recommends ITS and AFM management limit AirWatch and WASP system access to staff with a valid business need. We further recommend management formally approve, document, and periodically validate AirWatch and WASP system access rights. In addition, management should retain documentation of these control activities.	ITS will limit AirWatch access to ITS staff with specific job responsibilities inside that system. In addition, IT Security will review employee access to AirWatch and make policy changes on a quarterly basis. If changes are required for access to AirWatch, a Cherwell ticket will be opened, documented and approved by IT Security. Quarterly reports will be maintained by IT Security to document control activities.	09/2018	I (1) IO (4)	Internal Audit determined some control activities were not implemented and/or functioning as intended, e.g., approval and periodic review of access rights and formal documentation of control activities.
5.1	Internal Audit recommends ITS management separate incompatible duties or implement appropriate compensating controls to mitigate the risks.	ITS management will segregate duties of staff assigned to mobile device ordering, receiving and deployment.	12/2018	O	Management indicated the recommendation is open due to limited staff to perform these duties. ITS is working with Asset and Facility Management staff to begin receiving mobile equipment via WASP.
6.1	Internal Audit recommends ITS management provide routine staff oversight of the mobile device lifecycle, i.e., acquisition, storage/management, deployment, and retirement/disposal. In addition, Internal Audit recommends AFM management provide staff oversight of mobile device receiving, storage/management, and transfer to ITS. Both ITS and AFM	ITS management will provide internal oversight (periodic validation) of device lifecycles with documentation of reviews. The quarterly reports will be maintained by ITS security personnel.	12/2018	P (2)	Management indicated the recommendation is partially implemented due to the additional time needed to finalize several key activities, e.g., quarterly audit plans, final updates to the inventory system, and system-generated inventory reports.

Follow-Up Results
Information Technology Mobile Device Inventory Management Report 1662

- **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**
	management should retain documentation of their reviews.				