INTERNAL AUDIT DEPARTMENT

ALERT NUMBER 2014-002

AUDIT ALERT

JULY 23, 2014

WORKSPACE SECURITY

Workspace[1] security controls are necessary to minimize the potential risk of theft or misuse of confidential and sensitive data. Access to such information must be restricted to only those with a business need for it. Unattended sensitive documents and unlocked computers leave data vulnerable to abuse. We have recently observed employee workspaces left in this manner. Although it is not feasible for employees to remain at their workspaces continually, there are steps that can minimize the risk of inadvertently disclosing sensitive information.

This alert is being issued as a reminder of each employee's individual responsibility to keep information safeguarded. We all get busy in our jobs, but taking a few precautions can ensure workspaces remain secure.

Follow these tips to assist in maintaining proper workspace security:

- Lock your desktop, laptop, or wireless device each time you step away from your it.
- Keep documents with confidential or sensitive information in a locked desk or cabinet when not in use.
- Ensure documents with confidential data are discarded in a shredder or secure recycling bin once it is no longer needed.
- Keep external storage devices secure (i.e. thumb and zip drives).

- Lock your office door, if applicable.
- Avoid writing user IDs and passwords down; store them in a locked drawer if you must.
- Retrieve documents from the printer as soon as they are printed or use the secured print option.
- Log your computer off the network at the end of each day/shift.

NOTE: Personal items such as cell phones, purses, briefcases, etc. are also susceptible to theft. The above information can assist in properly securing those items as well.

For additional information, contact the Internal Audit Department.

[1] Space used or required for one's work (i.e. office, cubicle, vehicle, etc.)