1. Purpose

The purpose of this policy is to provide guidance for workstation security for People workstations in order to ensure the security of information on the workstation and information the workstation may have access to.

2. Scope

This policy applies to all People employees, contractors, workforce members, vendors and agents with a People-owned or personal-workstation connected to the People network.

3. Policy

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information.

4.1 Workforce members using workstations shall consider the sensitivity of the information that may be accessed and minimize the possibility of unauthorized access.
4.2 People will implement physical and technical safeguards for all workstations.
4.3 Appropriate measures include:

- Restricting physical access to workstations to only authorized personnel.
- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected. The password must comply with People *Password Policy*.
- Complying with all applicable password policies and procedures. See People *Password Policy*.
- Ensuring workstations are used for authorized business purposes only.
- Never installing unauthorized software on workstations.
- Keeping food and drink away from workstations in order to avoid accidental spills.
- Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
- Installing privacy screen filters or using other physical barriers to alleviate exposing data.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates.
- Exit running applications and close open documents
- Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
- If wireless network access is used, ensure access is secure by following the *Wireless Communication policy*

4. Policy Compliance

1. Compliance Measurement

The People Security Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

2. Exceptions

Any exception to the policy must be approved by the People Security Team in advance.

3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Revision History

Date of Change	Responsible	Summary of Change
June 2014	Sat Sindhar	Introduced policy
September 2014	People Sec Team	Small revisions to requirements