This assessment is used by supervisors, compensation specialists, HR business partners, recruiters and employees when considering transitioning an on-campus position to a hybrid or remote position. There are some jobs that are not suitable for a hybrid schedule or remote location, so it is important to carefully consider job function, workplace safety, and IT security.

### Reviewing Job Function

- Does the position have job functions that can be performed at a remote site without diminishing the quality of the work or disrupting the productivity of a unit?
- Does the position require an employee’s presence at the regularly assigned place of employment on a daily or routine basis?
- Does the position allow for an employee to be as effectively supervised as he or she would be if the job functions were performed at the assigned place of employment?
- Does the position have an emphasis on the electronic production and/or exchange of information by means of electronic equipment and reliable Internet?
- Does the position have a minimal or flexible need for specialized materials or equipment available only at the regularly assigned work site?

### Workplace Safety

- Does the employee have designated workspace at home that can be adequately equipped and complies with safety guidelines, as outlined in the Home Office Setup Guidelines?
- Will the employee reference Home Office Ergonomics information to aid in creating a comfortable workspace?
- Is the employee maintaining a safe home office space that includes the following?
  - An area free from hazards that can accommodate workspace equipment and related materials
  - Working smoke detectors, a usable fire extinguisher and an evacuation plan
  - Sufficient electrical outlets and a surge protector
  - Adequate temperature, ventilation and lighting

### IT Security

These policies and best practices or standards, identify the basic principles for protecting the confidentiality, integrity, and availability of University IT resources.

- Individuals are responsible for the security of computing devices under their control that interact with Purdue’s IT resources.
- All users must follow the measures outlined in the [Authentication, Authorization and Access Controls (S-13)] Standard and [End User Security Guidelines].
- Users must also adhere to any supplemental policies issued by departmental IT units and/or the owners of the IT resource(s) to be remotely accessed.
Remote Users accessing non-public University IT Resources must follow these requirements for any Remote Host accessing IT Resources, as well as any guidelines, procedures or other requirements issued by their departmental IT units and/or the owners of the IT Resource to be remotely accessed:

- Utilize Purdue’s VPN service to access IT Resources that are only available on campus.
- Utilize Purdue Career Account and Multi-factor Authentication service.
- Ensure the Remote Host meets the security expectations specified in the End User Security Guidelines.
- Take reasonable precautions to ensure Remote Access connections are secured from interceptions, eavesdropping or misuse including, but not limited to, shielding their screen from view in a public area when accessing sensitive or restricted data and not sharing the Remote Host with another party for use while it is remotely connected.
- Follow University Data Handling Procedures and any departmental requirements including, but not limited to, those associated with federal, state or local laws, such as HIPAA, FERPA, etc.