

## Appendix A - Employee Responsibilities

Employees should conduct themselves as representatives of both the DHHR and state government as a whole.

1. Employees will only access files, data, and protected records if:
  - a. the employee owns the information;
  - b. the employee is authorized to receive the information; or
  - c. the information is publicly available.
2. Employees are responsible for all activity that comes from their computer. For example, employees must:
  - a. always use strong passwords; and
  - b. NEVER share passwords with any individual for any reason
3. Employees must guard against access to files and take precautions to protect IT devices when away from the workstation. This will include but may not be limited to the following:
  - a. logging off computer;
  - b. locking computer; and/or
  - c. locking file drawers
4. Employees are prohibited from monopolizing systems; overloading networks with excessive data; or wasting computer time, connect time, bandwidth, disk space, printer paper, or other IT resources.
5. Employees are prohibited from transmitting personal information about themselves or someone else using state-provided IT resources without proper authorization.
6. Employees must report the following instances to a supervisor or appropriate authority:
  - a. receiving or obtaining information to which the employee is not entitled (Note: the owner or sender of such information must also be notified);
  - b. becoming aware of breaches in security; or
  - c. becoming aware of any inappropriate use of state-provided IT resource.
7. Employees will contact an immediate supervisor if there is doubt concerning authorization to access any state-provided IT resource.
8. Employees must adhere to copyright law regarding the use of software, print or electric information, and attributions of authorship.