

VII. Employee Responsibilities:

- a. It is the responsibility of all employees to follow the Information Systems and Security Policy. All judicial branch employees must also review IT security training materials each year to maintain compliance.
 - b. All employees are responsible for being security minded when dealing with passwords, hardware and state data. Passwords shall not be written down. Encrypted password keepers and training on how to use them can be provided by NSC-IT.
 - c. Employees should only login with their own credentials to any network or application. Sharing of login credentials is not allowed.
 - d. When an employee leaves his or her desk or computer, the employee will lock the device (Win+L).
 - e. An employee who is assigned technology equipment is responsible for safeguarding the equipment and controlling its use. Any employee whose equipment is mislaid or stolen should immediately report the loss or theft of such equipment to his or her supervisor and to the NSC-IT for proper incident reporting. If loss or damage of judicial branch owned equipment was caused by negligence on the part of the employee, the cost to replace or repair the item may be passed on to the employee. Upon separation from judicial branch employment, the employee is required to release any assigned equipment back to hiring manager or supervisor.
 - f. An employee who detects malware or any other compromise of the employee's device should immediately make a report to NSC-IT for proper incident reporting.
 - g. Employees will ensure that all removable media checked out to them will be secured at all times. Once an item of removable media has been used on a device not owned or leased by the judicial branch, it must be returned to NSC-IT for security scanning. Loss or theft of any item of removable media must be reported immediately to an employee's supervisor and NSC-IT.
 - h. Employees/contractors must utilize VPN whenever they are not directly connected to the state network. VPN must be used on any unsecured or public connection.
 - i. All judicial branch employees using state issued mobile devices must password protect the devices with a minimum of a 4-digit pin number. Stronger types of access control such as a longer password, thumbprint recognition are also acceptable. Personal mobile devices used to access state email must also adhere to the above guidelines.
-