✓**5. Security and Propriety Information**

All mobile and computing devices that connect to the internal network must comply with the Mobile Device and Teleworking Policy.

System-level and user-level passwords must comply with the Password Policy. Password sharing is strictly prohibited.

All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 5 minutes or less. You must lock the screen or log off when the device is unattended.

The Clear Screen and Clear Desk Policy must be adhered to at all times.

Registration to social media and newsgroups via use of your RRA work email is strictly prohibited. Exception to this rule includes select employees in Taxpayer Services who are authorized to make and respond to queries directed on RRA official social media pages.

Employees must exercise extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

✓**6. Unacceptable Use**

Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administrators may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of RRA authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing RRA-owned resources.

The following activities are strictly prohibited, unless if explicitly authorized or part of job description:

✓ 1.1. Violation of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use at RRA is prohibited.

✓1.2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which RRA or the end user does not have an active license is prohibited.

✓1.3. Installation and/or configuration of software without prior approval from the Head of IT Support and Helpdesk shall be prohibited. IT staff and/or IT Solution Providers under the supervision of IT staff are responsible for installing and supporting all software on any computers.

✓1.4. Accessing data, a server or an account for any purpose other than conducting RRA business, even if you have authorized access, is prohibited.

✓ 1.5. Introduction of malicious programs into RRA network or servers is strictly prohibited. Malicious programs or applications include but are not limited to viruses, worms, Trojan horses, e-mail bombs, etc. Detected viruses shall be immediately reported to the IT Team for prompt action to be taken.