✓1.6. Any portable media connected to any RRA computer (after formal approval) shall be scanned with antivirus software before accessing files on it.

✓1.7. Revealing your account password to others or allowing use of your account by others is prohibited. This includes family and other household members especially in situations where work is being done at home.

✓1.8. Using RRA information assets to actively engage in procuring or transmitting material that is in violation of sexual harassment or workplace laws in the user's local jurisdiction is prohibited.

✓1.9. Engaging in fraudulent activities at RRA, or making fraudulent offers of products, items, or services originating from any RRA accounts or systems is strictly prohibited.

✓1.10. Effecting security breaches or disruptions of network communications is prohibited. Security breaches include, but are not limited to, accessing data for which the employee is not an intended recipient, logging into a server or account that the employee is not expressly authorized to access, etc. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

✓1.11. Port scanning or security scanning is expressly prohibited unless prior authorization to do so has been given, and the activities pose no danger to RRA information systems.

✓1.12. Executing any form of network monitoring that will intercept data not intended for an employee's host is strictly prohibited, unless if this activity is part of the employee's duties and he/she has been authorized to do so.

✓1.13. Circumventing user authentication or security of any host, network or account is prohibited.

✓1.14. Introducing honeypots, honey nets, or similar technology on the RRA network is not allowed.

✓1.15. Interfering with or denying service to any legitimate RRA user in a manner that prevents him or her from performing legitimate business duties or functions is strictly prohibited e.g., denial of service attack.

✓1.16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet is prohibited.

✓1.17. Providing proprietary information to parties outside RRA in a manner that violates RRA's information security policy and information classification standard is strictly prohibited.

✓7. **Blogging and Social Networking sites**

✓1.18. All internet use from RRA's systems is potentially subject to monitoring.

✓1.19. Employees browsing social media and blogging sites while using RRA systems/resources, or personal computers on RRA controlled networks, are subject to the terms and restrictions set forth in this policy.