



United States Department of Agriculture

Office of the
Secretary

Office of the Chief
Information Officer

1400 Independence
Avenue S.W.

Washington, DC
20250

TO: Assistant Chief Information Officers
Chiefs of Staff
Chief Operating Officers
Chief Human Capital Officers

FROM: Gary S. Washington
Chief Information Officer

SUBJECT: Information Technology Improper Use Guidance

In accordance with Departmental Regulation (DR) 3300-001 *Telecommunications & Internet Services and Use* and Departmental Manual (DM) 3525, *Internet Use and Copyright Restrictions*, all users of the U.S. Department of Agriculture (USDA) Information Technology (IT) are expected to utilize official government IT equipment for official use and authorized purposes only. Access agreements (e.g., acceptable use agreement, non-disclosure agreement, and rules of behavior) guide permissible and non-permissible actions personnel may perform on USDA information systems. All USDA personnel (i.e., USDA employees, contractors, affiliates, interns, fellows, and volunteers) must acknowledge their understanding of the access agreements prior to being granted access to information systems.

The following specific activities are prohibited on any USDA information system:

1. Unauthorized modifying, or attempting to modify, information security controls;
2. Downloading unauthorized software, such as peer-to-peer, illegal or copyrighted material, or distributing illegally obtained files or software;
3. Activities that are inappropriate or offensive (accessing sexually explicit materials, hate speech, or remarks ridiculing others based on race, color, national origin, religion, sex, gender identity (including gender expression), sexual orientation, disability, age, marital status, family/parental status, income derived from a public assistance program, political beliefs, or reprisal or retaliation for prior civil rights activity);
4. Accessing or attempting to access systems for unauthorized purposes, including, but not limited to invasion of privacy, snooping, obtaining information the user is not authorized to access;
5. Permitting or enabling unauthorized personnel to access a USDA information system;
6. Gambling or activities that relate to any type of outside employment;
7. Viewing and downloading material of a pornographic nature;
8. Political activity including campaigning, lobbying Congress, or any government agency;
9. Any type of continuous audio or video streaming from commercial, private, news, or financial organizations;
10. Endorsement of any non-government products, services, or organizations; and
11. The use of Apps such as: Telegram, WhatsApp, and Facebook Messenger.

Improper use of USDA systems and data may result in appropriate administrative action. DR 4070-735-001, *Employee Responsibilities and Conduct*, Section 21, states that a violation of any of the responsibilities and conduct standards contained in USDA directives related to use of government systems and equipment may be cause for disciplinary action. Incidents involving suspected criminal activity will be referred to the Office of the Inspector General (OIG).

Please ensure compliance with all rules and regulations regarding improper use. We also request that you report suspicious activity or violations to appropriate management and supervisory personnel. For more information or to report an incident, please contact the Information Security Center (ISC) 24 Hour Hotline at: cyber.incidents@usda.gov or 866.905.6890.

cc: Mary Pletcher