**COUNTY OF ORANGE, VIRGINIA**
**PERSONNEL POLICIES MANUAL**

# ACCEPTABLE USE POLICY

**POLICY NO.: 3.11** **EFFECTIVE:** 1/10/17
**REVISED:**

---

**OVERVIEW:** The Information Technology Department's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Orange County's established culture of openness, trust, and integrity. The Information Technology Department is committed to protecting Orange County's employees, partners, and the organization from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including, but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Orange County. These systems are to be used for business purposes in serving the interests of the organization, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Orange County employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

**PURPOSE:** The purpose of this policy is to outline the acceptable use of computer equipment in Orange County. These rules are in place to protect the employee and the County. Inappropriate use exposes Orange County to risks, including virus attacks, compromise of network systems and services, and legal issues.

**SCOPE:** This policy applies to the use of information, electronic and computing devices, and network resources to conduct Orange County business or interact with internal networks and business systems, whether owned or leased by Orange County, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers in Orange County and its subsidiaries are responsible for exercising good judgment regarding the appropriate use of information, electronic devices, and network resources in accordance with Orange County policies and standards, and local laws and regulation.

This policy applies to employees, contractors, consultants, temporary, and other workers in Orange County, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Orange County.

**PROVISIONS:**

A. General Use and Ownership

1. Orange County proprietary information stored on electronic and computing devices, whether owned or leased by Orange County, the employee, or a third party, remains the sole property of Orange County. You must ensure, through legal or technical means, that proprietary information is protected.

2. You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Orange County proprietary information.

3. You may access, use, or share Orange County proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and, if there is any uncertainty, employees should consult their supervisor or manager.

5. For security and network maintenance purposes, authorized individuals within Orange County may monitor equipment, systems, and network traffic at any time.

6. Orange County reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

7. Orange County may track and/or review all Internet/Intranet/Extranet use, and may maintain logs of such use.

B. Security and Proprietary Information

1. System level and user level passwords must comply with Policy 3.11.A (Password Policy). Providing access to another individual, either deliberately or through failure to secure access, is prohibited.

2. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to ten (10) minutes or less. You must lock the screen or log off when the device is unattended.

3. Postings by employees from an Orange County email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Orange County, unless posting is in the course of business duties.

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

C. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g.: systems administration staff 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 Orange County authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing Orange County-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

1. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

a. Violations 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 by Orange County.

b. 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 Orange County or the end user does not have an active license.

c. Accessing data, a server, or an account for any purpose other than conducting Orange County business, even if you have authorized access.

d. Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

e. Introduction of malicious programs into the network or server (e.g.: viruses, worms, Trojan horses, e-mail bombs, etc.).

f. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being conducted at home.

g. Using an Orange County computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

h. Viewing pornography or any type of sexually explicit material.

i. Trolling or otherwise posting offensive comments on websites.

j. Making fraudulent offers of products, items, or services originating from any Orange County account.

k. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

l. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. 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.

m. Port scanning or security scanning, unless prior notification to the Information Technology Department is made.

n. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duties.

o. Circumventing user authentication or security of any host, network, or account.

p. Introducing honeypots, honeynets, or similar technology on the Orange County network.

q. Interfering with or denying service to any user other than the employee's host (for example: denial of service attack).

r. 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.

2. Email and Communication Activities

When using organization resources to access and use the Internet, users must realize they represent the County. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company." Questions may be addressed to the Information Technology Department.

a. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material, to individuals who did not specifically request such material ("spam").

b. Any form of harassment via e-mail, telephone, or paging, whether through language, frequency, or size of messages.

c. Unauthorized use, or forging, of e-mail header information.

d. Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.

e. Creating or forwarding "chain letters," "Ponzi," or other "pyramid" schemes of any kind.

f. Use of unsolicited e-mail originating from within Orange County's networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Orange County or connected via Orange County's network.

g. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups ("newsgroup spam").

3. Blogging and Social Media Activities

a. Blogging by employees, whether using Orange County's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Orange County's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Orange County's policy, is not detrimental to Orange County's best interests, and does not interfere with an employee's regular job duties. Blogging from Orange County's systems is also subject to monitoring.

b. Orange County's policies related to confidential and proprietary information also apply to blogging. As such, employees are prohibited from revealing any Orange County confidential or proprietary information, trade secrets, or any other material covered by Orange County's policies when engaged in blogging.

c. Employees shall not engage in any blogging that may harm or tarnish the image, reputation, and/or goodwill of Orange County and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory, or harassing comments when blogging or otherwise engaging in any conduct prohibited by Orange County Policy 1.2 (Equal Opportunity Statement) and Policy 3.1 (Sexual and Other Unlawful Harassment).

d. Employees may also not attribute personal statements, opinions, or beliefs to Orange County when engaged in blogging. If an employee is expressing his or her

beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Orange County. Employees assume any and all risk associated with blogging.

e. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Orange County's trademarks, logos, and any other Orange County intellectual property may also not be used in connection with any blogging activity.

D. Policy Compliance

1. Compliance Measurement

The Information Technology Department will verify compliance to this policy through various methods, including, but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

2. Exceptions

Any exception to this Policy must be approved by the Information Technology Department or County Administrator in advance.

3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.