Policy Title and #	CIO-061: Social Media Policy				
Effective Date:	7/1/2011	Revision Date:	01/11/2023	Review Date:	01/11/2023

POLICY STATEMENT

This policy establishes controls related to Commonwealth Office of Technology (COT) Enterprise requirements for Social Media use. The policy provides guidance in decision-making and practices that optimize resources, mitigate project risk, and maximize return on investments.

DEFINITION

Social Media: Technologies and platforms that allow users and organizations to create and share information via communities and networks. The media may share information globally (e.g., Facebook or YouTube), or organizations may use the media internally (e.g., internal SharePoint sites).

POLICY

COT and agencies have an opportunity and obligation to communicate with the public about their services, events, plans, and other business information. Social Media, such as Facebook, Twitter, or YouTube provides agencies additional, cost-effective ways to communicate information. Social Media, when coupled with traditional information dissemination channels, can enhance an agency's outreach and communication with the public. This policy outlines the IT requirements needed to address the opportunities and risks concerning the use of Social Media. The policy only addresses the Social Media platforms used for external, public-facing communications.

Agencies shall:

- Use only official agency-branded accounts. No personal accounts may be used to communicate official agency business, and no official accounts may be used for personal opinions or information.
- Establish, maintain, and secure information related to agency Social Media accounts. Agencies must safeguard this information against compromise, as well as ensuring the availability and continued access to the accounts in the event of an emergency, employee termination, and retirement.
- Ensure that official Social Media accounts address appropriate security and compliance requirements, including account password changes and password complexity constraints.
- Ensure that the agency's use of Social Media complies with:
    - CIO-060 Acceptable Use Policy
    - CIO-071 Wireless Voice and Data Services Policy
    - CIO-092 Media Protection Policy
    - CIO-093 Risk Assessment Policy
    - Agency policies concerning official communications and the release of information by the agency
    - Terms of Service for each Social Media platform in use by the agency.

Agencies shall **not**:

- Release non-public information, such as personal, sensitive, confidential, or other personally identifiable information. The agency shall comply with all requirements for the release of any public information by use of Social Media.
- Release information concerning litigation or potential litigation.
- Release any content that violates any state or federal statute, regulation, or internal procedure.
- Release any information in violation of copyright, fair use, and other applicable intellectual property laws.
- Use an application or otherwise access the Social Media site owned by the Chinese company ByteDance Limited or its successors commonly known as "Tik Tok," other than for a law enforcement purpose;
- Release any Federal Tax Information by use of Social Media.

This policy is subject to all terms and provisions of the ENT-301 Acceptable Use and Social Media Guidelines, all of which are, by this reference made a part of and incorporated in this policy.

Agency staff who fail to comply with policies concerning Social Media are subject to agency disciplinary action, up to and including dismissal.

Agencies may request exceptions to this policy by submitting a security exemption request via the Commonwealth Office of Technology ticketing system. The CISO will consider requests on a case-by-case basis. COT may pass any costs resulting from the exemptions or exceptions to this policy to those agencies.

AUTHORITY
KRS 42.726 authorizes the Commonwealth Office of Technology (COT) to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

APPLICABILITY
All executive branch agencies and non-executive branch agencies using COT-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

RESPONSIBILITY FOR COMPLIANCE
Each agency shall ensure that staff within their organizational authority are made aware of and comply with this policy. The agency is responsible for enforcing it. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. COT may require additional service charges for remediation efforts due to non-compliance with this policy.

MAINTENANCE
COT's Office of Contracts and Privacy is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

REFERENCES

Helpful references can be found on the Enterprise IT Policies webpage.