



WSU POLICY APPROVAL COVER PAGE

	[INSERT DATE]
	19.19 / Prohibited Use of TikTok and Similar Applications
	N/A
	N/A
	Office of General Counsel and Information Security
<p>This new policy sets forth the University's prohibitions on the use of TikTok and similar applications provided by ByteDance Limited on the University's network and on any electronic device that is used in the performance of a federal government grant or contract.</p>	
<p>In June 2023, the federal government issued a new rule, Federal Acquisition Regulation, 48 C.F.R. 52.204–27, which prohibits the presence or use of any application or service developed or provided by ByteDance Limited, including the social networking service TikTok, on any information technology equipment used in the performance of a federal contract. The purpose of this policy is to formalize and further clarify the prohibitions that the University has already put in place to ensure compliance with the new federal rule.</p>	
<p>Consolidated Appropriations Act, December 23, 2023, Pub. L. No. 117-328, div. R, §§ 101-02, No TikTok on Government Devices Act</p> <p>FAR 52.204-27 Prohibition on a ByteDance Covered Application</p> <p>FAR 4.2203 Contract clause</p> <p>Memorandum M-23-13, "No TikTok on Government Devices" Implementation Guidance, issued by the Office of Management and Budget on February 27, 2023</p>	
	Office of the General Counsel – Stacia Boden and Misha Jacob-Warren
	Information Security – Mark Rodee
	IDP Information Security – Chris Snyder

	IDP Information Security – Jeff Westeman
	Staff Senate – Jason Bosch (shared) [PENDING]
	Faculty Senate – Jolynn Dowling

19.19 / PROHIBITED USE OF TIKTOK geNSc 0Γw 2023

- 4. **Electronic Device:** Any mobile communication device, including but not limited to a cell phone, pager, laptop, tablet, or any other electronic device that is used for communication or data storage. This policy applies to all employees, regardless of their position or location. Employees are prohibited from using these devices for personal use during work hours. If an employee is using a mobile device for work purposes, they must ensure that all data is encrypted and that the device is protected by a password or other security measure. Employees are also prohibited from installing any software or applications on their work devices without the approval of the IT department.
- 5. **Employee:** Any individual who is employed by the organization. This policy applies to all employees, regardless of their position or location. Employees are prohibited from using their work email accounts for personal use. Employees are also prohibited from installing any software or applications on their work devices without the approval of the IT department.
- 6. **Leadership:** Any individual who is in a leadership position within the organization. This policy applies to all employees, regardless of their position or location. Employees are prohibited from using their work email accounts for personal use. Employees are also prohibited from installing any software or applications on their work devices without the approval of the IT department.
- 7. **Personal Electronic Device:** Any mobile communication device, including but not limited to a cell phone, pager, laptop, tablet, or any other electronic device that is used for communication or data storage. This policy applies to all employees, regardless of their position or location. Employees are prohibited from using these devices for personal use during work hours. If an employee is using a mobile device for work purposes, they must ensure that all data is encrypted and that the device is protected by a password or other security measure. Employees are also prohibited from installing any software or applications on their work devices without the approval of the IT department.

- B. FAIR 48 C.F.R. 52.20427, PhDa
Ca
- C. FAIR 48 C.F.R. 4.2203, Ca
- D. M 11 -23-13, NoGdIn
Guidance Bu 27, 2023

VI. REVISION DATES

- A. [INSERT APPROX L DAE]