

**SUBSTITUTE FOR
HOUSE BILL NO. 4235**

A bill to prohibit the use of certain applications on government-issued devices; to require public employers to take certain actions related to prohibited applications; to prohibit certain employees or officers from downloading or accessing certain applications; to provide exceptions; and to provide for the powers and duties of certain state and local governmental officers and entities.

THE PEOPLE OF THE STATE OF MICHIGAN ENACT:

1 Sec. 1. This act may be cited as the "prohibited applications
2 on government-issued devices act".

3 Sec. 3. The legislature finds that a proper and legitimate
4 state purpose is served when efforts are taken to secure the
5 system, network, or server of a public employer. Therefore, the

1 legislature determines and declares that this act fulfills an
2 important state interest.

3 Sec. 5. As used in this act:

4 (a) "Department" means the department of technology,
5 management, and budget.

6 (b) "Employee or officer" means an individual who performs
7 labor or services for a public employer for salary, wages, or other
8 remuneration.

9 (c) "Foreign country of concern" means any of the following:

10 (i) The People's Republic of China.

11 (ii) The Russian Federation.

12 (iii) The Islamic Republic of Iran.

13 (iv) The Democratic People's Republic of Korea.

14 (v) The Republic of Cuba.

15 (vi) The Venezuelan regime of Nicolás Maduro.

16 (vii) The Syrian Arab Republic.

17 (viii) Any agency of or any other entity under significant
18 control of an entity listed under subdivisions (i) to (vii).

19 (d) "Foreign principal" means any of the following:

20 (i) The government or an official of the government of a
21 foreign country of concern.

22 (ii) A political party, a member of a political party, or any
23 subdivision of a political party in a foreign country of concern.

24 (iii) A partnership, an association, a corporation, an
25 organization, or a combination of persons organized under the laws
26 of or having its principal place of business in a foreign country
27 of concern, or an affiliate or a subsidiary of a partnership, an
28 association, a corporation, an organization, or a combination of
29 persons organized under the laws of or having its principal place

1 of business in a foreign country of concern.

2 (iv) Any individual who is domiciled in a foreign country of
3 concern and is not a citizen or a lawful permanent resident of the
4 United States.

5 (e) "Government-issued device" means a cellular telephone, a
6 desktop computer, a laptop computer, or other electronic device
7 that is capable of connecting to the internet owned or leased by a
8 public employer and issued to an employee or officer for work-
9 related purposes.

10 (f) "Prohibited application" means an internet application
11 that meets the following criteria:

12 (i) The internet application is created, maintained, or owned
13 by a foreign principal and participates in activities that include,
14 but are not limited to, any of the following:

15 (A) Collects keystrokes or sensitive personal, financial,
16 proprietary, or business data.

17 (B) Compromises emails and acts as a vector for ransomware
18 deployment.

19 (C) Conducts cyber-espionage against a public employer.

20 (D) Conducts surveillance and tracks individual users.

21 (E) Uses algorithmic modifications to conduct disinformation
22 or misinformation campaigns.

23 (ii) The department considers the internet application to
24 present a security risk in the form of unauthorized access to or
25 temporary unavailability of the public employer's records, digital
26 assets, systems, networks, servers, or information.

27 (g) "Public employer" means this state, a local unit of
28 government or other political subdivision of this state, any
29 intergovernmental, metropolitan, or local department, agency, or

1 authority, or other local political subdivision, a school district,
2 a public school academy, or an intermediate school district, as
3 those terms are defined in sections 4 to 6 of the revised school
4 code, 1976 PA 451, MCL 380.4 to 380.6, a community college or
5 junior college described in section 7 of article VIII of the state
6 constitution of 1963, or an institution of higher education
7 described in section 4 of article VIII of the state constitution of
8 1963.

9 Sec. 7. (1) Except as otherwise provided in subsection (3), a
10 public employer shall do all of the following:

11 (a) Block a prohibited application from public access on any
12 network and virtual private network owned, operated, or maintained
13 by that public employer.

14 (b) Restrict access to any prohibited application on a
15 government-issued device.

16 (c) Retain the ability to remotely wipe and uninstall any
17 prohibited application from a government-issued device that is
18 believed to have been adversely impacted, either intentionally or
19 unintentionally, by a prohibited application.

20 (2) A person, including an employee or officer, shall not
21 download or access a prohibited application on a government-issued
22 device. This subsection does not apply to a law enforcement officer
23 if the use of the prohibited application is necessary to protect
24 the public safety or conduct an investigation within the scope of
25 the law enforcement officer's employment.

26 (3) A public employer may request a waiver from the department
27 to allow a designated employee or officer to download or access a
28 prohibited application on a government-issued device. A request for
29 a waiver under this subsection must be in writing and include all

1 of the following:

2 (a) A description of the activity to be conducted and the
3 state interest furthered by the activity.

4 (b) The maximum number of government-issued devices and
5 employees or officers to which the waiver will apply.

6 (c) The length of time necessary for the waiver. A waiver
7 granted under this subsection must be limited to a time frame of
8 not more than 1 year, but the department may approve an extension.

9 (d) Risk mitigation actions that will be taken to prevent
10 access to sensitive data, including methods to ensure that the
11 activity does not connect to a state system, network, or server.

12 (e) A description of the circumstances under which the waiver
13 applies.

14 Sec. 9. (1) Not later than 90 days after the effective date of
15 this act, the department shall do both of the following:

16 (a) Compile and maintain a list of all prohibited
17 applications, and publish the list on its website. The department
18 shall update the list compiled and maintained under this
19 subdivision quarterly, and provide notice of any update to all
20 public employers.

21 (b) Establish procedures for granting or denying a waiver
22 under section 7(3).

23 (2) Not later than 15 calendar days after the department
24 issues or updates the list of prohibited applications under
25 subsection (1)(a), an employee or officer who uses a government-
26 issued device must remove, delete, or uninstall any prohibited
27 application on the list of prohibited applications from the
28 employee's or officer's government-issued device.

29 Sec. 11. The department shall promulgate rules to implement

1 this act under the administrative procedures act of 1969, 1969 PA
2 306, MCL 24.201 to 24.328.

3 Enacting section 1. This act takes effect December 31, 2025.