60GG-2.0075 Unmanned Aerial Systems (UAS) Minimum Security Requirements.

(1) Definitions.

(a) "Critical Component" means a Drone component related to: flight controllers, radio, data transmission devices, cameras, gimbals, ground control systems, operating software (including cell phone or tablet applications, but not cell phone or tablet operating systems), network connectivity, or data storage. Critical Components do not include, for example, passive electronics such as resistors, and non-data transmitting motors, batteries, and wiring.

(b) "Data" means any electronic information of a Governmental Agency that is a public record, as defined in Section 119.011(12), F.S.

(c) "Drone" has the same meaning as provided in Section 934.50(2)(a), F.S.

(d) "Florida College System Institution" has the same meaning as provided in Section 1000.21(3), F.S.

(e) "Foreign Country of Concern" has the same meaning as provided in Section 286.101(1)(b), F.S.

(f) "Governmental Agency" has the same meaning as provided in Section 934.50(7)(a)2., F.S.

(g) "Instructional Technology" means an interactive device used by a School that assists in instructing a class or a group of students and includes the necessary hardware and software to operate the interactive device. The term also includes support systems in which an interactive device may mount and is not required to be affixed to the facilities.

(h) "Open Data" means Data that is structured in a way that enables the Data to be fully discoverable and usable by the public. The term does not include Data that are restricted from public disclosure based on federal or state laws and regulations, including, but not limited to, those related to privacy, confidentiality, security, personal health, business or trade secret information, and exemptions from state public records laws; or Data for which a Governmental Agency is statutorily authorized to assess a fee for its distribution.

(i) "Research and Accountability Purposes" means Drone use by a Florida College System Institution or a State University in direct support of research on Drone hardware, operating systems, software, communications systems and protocols, components, and data practices for the purpose of understanding the existence and extent of potential threats and vulnerabilities, and mitigations thereto. This research must be conducted at the direction of a state of Florida agency or a federal agency, or a party contracted by a state of Florida agency or a federal agency to conduct the research.

(j) "School" has the same meaning as provided in Section 1003.01(2), F.S.

(k) "State University" has the same meaning as provided in Section 1000.21(6), F.S.

(2) Approved Manufacturers. A Governmental Agency may only use a Drone from a manufacturer that meets the minimum security requirements specified in this rule. A manufacturer that meets such requirements is deemed an approved manufacturer for the given tier as specified in subsection (3). Notwithstanding a manufacturer's designation as an approved manufacturer, the Governmental Agency is still required to ensure that the Drone it intends to use complies with all applicable provisions of this rule.

(3) Tiers.

Tiers and Exceptions	**Description**	**Applicable Minimum Security Requirements**
Tier One	A Drone that does not collect, transmit, or receive Data during flight. Examples of such Drones include Drones that navigate along pre-programmed waypoints and tethered Drones. A Drone used by a School exclusively as Instructional Technology shall be classified as Tier One Drone use.	Subsection (4), Foreign Countries of Concern; subsection (5), Standard Precautions.
Tier Two	A Drone that may collect, transmit, or receive only flight control Data, excluding visual and auditory Data.	Subsection (4), Foreign Countries of Concern; subsection (5), Standard Precautions; subsection (6), Tier Two.
Tier Three	A Drone that may collect, transmit, or receive any Data, including visual and auditory Data.	Subsection (4), Foreign Countries of Concern; subsection (5), Standard Precautions; subsection (6), Tier Two; subsection (7), Tier Three.
Research and Accountability Purposes Exception	Drones used for Research and Accountability Purposes are exempt from the requirements in subsection (4), (6), and (7). If using otherwise prohibited Drones for Research and Accountability	Subsection (5), Standard Precautions.

	Purposes, the Governmental Agency should weigh the goals of the research against the risk to networks and Data. A Governmental Agency using otherwise prohibited Drones under this exception must provide written notice to the Department of such use via email to drones@dms.fl.gov no later than 30 days prior to utilizing the exception. Such notice must state the intended purpose, participants, and ultimate beneficiaries of the research. To the extent allowable by law and existing agreement between the parties to the research, the State University or Florida College System Institution conducting research under this exception must, upon request of the Department, provide access to the research findings.	

(4) Foreign Countries of Concern. A Governmental Agency may not purchase, acquire, or otherwise use a Drone or any related services or equipment produced by a manufacturer domiciled in, or produced by a manufacturer the Governmental Agency reasonably believes to be owned or controlled (in whole or in part) by, a Foreign Country of Concern.

(5) Standard Precautions. A Drone or its software in use by a Governmental Agency:

(a) Shall only connect to the internet for purposes of command and control, coordination, or other communication to ground control stations or systems related to the mission of the Drone. If connecting to the internet under this paragraph, a Governmental Agency shall:

1. Require the command and control, coordination, or other ground control stations or systems to be secured and monitored; or

2. Require the command and control, coordination, or other ground control stations or systems to be isolated from networks where the Data of a Governmental Agency is held (e.g., air-gapping).

(b) Shall only connect to a computer or the network of a Governmental Agency if:

1. A Drone or its software is isolated in a way that prevents access to the internet and any network where the Data of a Governmental Agency is held;

2. A Drone or its software uses removable memory to connect to a computer or network that is isolated in a way that prevents access to any network where the Data of a Governmental Agency is held; and

3. Any transfer of Data between an isolated network described in subparagraphs 1. and 2. and a network where the Data of a Governmental Agency is held requires:

a. an initial scan using antivirus or anti-malware software for malicious code on the computer that connected directly or indirectly to the Drone;

b. the use of antivirus and anti-malware software during Data transfer; and

c. a scan of the destination of the transferred Data using antivirus or anti-malware software for malicious code.

(c) Shall not connect with a telephone, tablet, or other mobile device issued by a Governmental Agency or that connects to a Governmental Agency network. Governmental Agency devices that are solely used for the command and control, coordination, or other communication to ground control stations or systems related to the mission of the of Drones that do not connect to the Governmental Agency's network may be used.

(d) Shall be used in compliance with all other applicable Data standards as required by law and the Governmental Agency's own policy and procedure.

(6) Tier Two. A Drone or any related services or equipment used in accordance with Tier Two must, in addition to the requirements in paragraphs (4) and (5), meet the following minimum security requirements:

(a) Regardless of whether the Governmental Agency is an “agency” as defined in Rule 60GG-2.001, F.A.C., the Governmental Agency must comply with the portions of Rules 60GG-2.002, 60GG-2.003, and 60GG-2.004, F.A.C., that would by their nature be applicable to Drone use, its software, or any related services or interacting with any Data originating from the Drone or its use.

(b) All communication to and from a Drone shall utilize a Federal Information Process Standard (FIPS) 140-2 compliant encryption algorithm.

(c) Critical Components may not be produced by a manufacturer domiciled in, or produced by a manufacturer the Governmental Agency reasonably believes to be owned, controlled by, or otherwise connected to, a Foreign Country of Concern.

(7) Tier Three. A Drone or any related services or equipment used in accordance with Tier Three must, in addition to the requirements in subsections (4), (5), and (6), meet the following minimum security requirements:

(a) Data storage must be restricted to the geographic location of the continental United States. Remote access to Data storage, other than Open Data, from outside the continental United States, is prohibited unless approved in writing by the Governmental Agency head or designee.

Rulemaking Authority 934.50 FS. Law Implemented 934.50 FS. History–New 4-5-23.