

2016624er

1
2 An act relating to public records; amending s.
3 282.318, F.S.; creating exemptions from public records
4 requirements for certain records held by a state
5 agency which identify detection, investigation, or
6 response practices for suspected or confirmed
7 information technology security incidents and for
8 certain portions of risk assessments, evaluations,
9 external audits, and other reports of a state agency's
10 information technology program; authorizing disclosure
11 of confidential and exempt information to certain
12 agencies and officers; providing for retroactive
13 application; providing for future legislative review
14 and repeal of the exemptions; providing statements of
15 public necessity; providing an effective date.

16
17 Be It Enacted by the Legislature of the State of Florida:

18
19 Section 1. Paragraph (i) of subsection (4) of section
20 282.318, Florida Statutes, is amended, present subsection (5) of
21 that section is renumbered as subsection (6), and a new
22 subsection (5) is added to that section, to read:

23 282.318 Security of data and information technology.—

24 (4) Each state agency head shall, at a minimum:

25 (i) Develop a process for detecting, reporting, and
26 responding to threats, breaches, or information technology
27 security incidents which is ~~that are~~ consistent with the
28 security rules, guidelines, and processes established by the
29 Agency for State Technology.

2016624er

30 1. All information technology security incidents and
31 breaches must be reported to the Agency for State Technology.

32 2. For information technology security breaches, state
33 agencies shall provide notice in accordance with s. 501.171.

34 3. Records held by a state agency which identify detection,
35 investigation, or response practices for suspected or confirmed
36 information technology security incidents, including suspected
37 or confirmed breaches, are confidential and exempt from s.
38 119.07(1) and s. 24(a), Art. I of the State Constitution, if the
39 disclosure of such records would facilitate unauthorized access
40 to or the unauthorized modification, disclosure, or destruction
41 of:

42 a. Data or information, whether physical or virtual; or

43 b. Information technology resources, which includes:

44 (I) Information relating to the security of the agency's
45 technologies, processes, and practices designed to protect
46 networks, computers, data processing software, and data from
47 attack, damage, or unauthorized access; or

48 (II) Security information, whether physical or virtual,
49 which relates to the agency's existing or proposed information
50 technology systems.

51
52 Such records shall be available to the Auditor General, the
53 Agency for State Technology, the Cybercrime Office of the
54 Department of Law Enforcement, and, for state agencies under the
55 jurisdiction of the Governor, the Chief Inspector General. Such
56 records may be made available to a local government, another
57 state agency, or a federal agency for information technology
58 security purposes or in furtherance of the state agency's

2016624er

59 official duties. This exemption applies to such records held by
60 a state agency before, on, or after the effective date of this
61 exemption. This subparagraph is subject to the Open Government
62 Sunset Review Act in accordance with s. 119.15 and shall stand
63 repealed on October 2, 2021, unless reviewed and saved from
64 repeal through reenactment by the Legislature.

65 (5) The portions of risk assessments, evaluations, external
66 audits, and other reports of a state agency's information
67 technology security program for the data, information, and
68 information technology resources of the state agency which are
69 held by a state agency are confidential and exempt from s.
70 119.07(1) and s. 24(a), Art. I of the State Constitution if the
71 disclosure of such portions of records would facilitate
72 unauthorized access to or the unauthorized modification,
73 disclosure, or destruction of:

74 (a) Data or information, whether physical or virtual; or

75 (b) Information technology resources, which include:

76 1. Information relating to the security of the agency's
77 technologies, processes, and practices designed to protect
78 networks, computers, data processing software, and data from
79 attack, damage, or unauthorized access; or

80 2. Security information, whether physical or virtual, which
81 relates to the agency's existing or proposed information
82 technology systems.

83
84 Such portions of records shall be available to the Auditor
85 General, the Cybercrime Office of the Department of Law
86 Enforcement, the Agency for State Technology, and, for agencies
87 under the jurisdiction of the Governor, the Chief Inspector

2016624er

88 General. Such portions of records may be made available to a
89 local government, another state agency, or a federal agency for
90 information technology security purposes or in furtherance of
91 the state agency's official duties. For purposes of this
92 subsection, "external audit" means an audit that is conducted by
93 an entity other than the state agency that is the subject of the
94 audit. This exemption applies to such records held by a state
95 agency before, on, or after the effective date of this
96 exemption. This subsection is subject to the Open Government
97 Sunset Review Act in accordance with s. 119.15 and shall stand
98 repealed on October 2, 2021, unless reviewed and saved from
99 repeal through reenactment by the Legislature.

100 Section 2. (1) (a) The Legislature finds that it is a public
101 necessity that public records held by a state agency which
102 identify detection, investigation, or response practices for
103 suspected or confirmed information technology security
104 incidents, including suspected or confirmed breaches, be made
105 confidential and exempt from s. 119.07(1), Florida Statutes, and
106 s. 24(a), Article I of the State Constitution if the disclosure
107 of such records would facilitate unauthorized access to or the
108 unauthorized modification, disclosure, or destruction of:

109 1. Data or information, whether physical or virtual; or

110 2. Information technology resources, which includes:

111 a. Information relating to the security of the agency's
112 technologies, processes, and practices designed to protect
113 networks, computers, data processing software, and data from
114 attack, damage, or unauthorized access; or

115 b. Security information, whether physical or virtual, which
116 relates to the agency's existing or proposed information

2016624er

117 technology systems.

118 (b) Such records shall be made confidential and exempt for
119 the following reasons:

120 1. Records held by a state agency which identify
121 information technology detection, investigation, or response
122 practices for suspected or confirmed information technology
123 incidents or breaches are likely to be used in the investigation
124 of the incident or breach. The release of such information could
125 impede the investigation and impair the ability of reviewing
126 entities to effectively and efficiently execute their
127 investigative duties. In addition, the release of such
128 information before completion of an active investigation could
129 jeopardize the ongoing investigation.

130 2. An investigation of an information technology security
131 incident or breach is likely to result in the gathering of
132 sensitive personal information, including identification numbers
133 and personal financial and health information not otherwise
134 exempt or confidential and exempt from public records
135 requirements under any other law. Such information could be used
136 for the purpose of identity theft or other crimes. In addition,
137 release of such information could subject possible victims of
138 the incident or breach to further harm.

139 3. Disclosure of a record, including a computer forensic
140 analysis, or other information that would reveal weaknesses in a
141 state agency's data security could compromise the future
142 security of that agency or other entities if such information
143 were available upon conclusion of an investigation or once an
144 investigation ceased to be active. The disclosure of such a
145 record or information could compromise the security of state

2016624er

146 agencies and make those state agencies susceptible to future
147 data incidents or breaches.

148 4. Such records are likely to contain proprietary
149 information about the security of the system at issue. The
150 disclosure of such information could result in the
151 identification of vulnerabilities and further breaches of that
152 system. In addition, the release of such information could give
153 business competitors an unfair advantage and weaken the position
154 of the entity supplying the proprietary information in the
155 marketplace.

156 5. The disclosure of such records could potentially
157 compromise the confidentiality, integrity, and availability of
158 state agency data and information technology resources, which
159 would significantly impair the administration of vital
160 governmental programs. It is necessary that this information be
161 made confidential in order to protect the technology systems,
162 resources, and data of state agencies. The Legislature further
163 finds that this public records exemption be given retroactive
164 application because it is remedial in nature.

165 (2) (a) The Legislature also finds that it is a public
166 necessity that portions of risk assessments, evaluations,
167 external audits, and other reports of a state agency's
168 information technology security program for the data,
169 information, and information technology resources of the state
170 agency which are held by a state agency be made confidential and
171 exempt from s. 119.07(1), Florida Statutes, and s. 24(a),
172 Article I of the State Constitution if the disclosure of such
173 portions of records would facilitate unauthorized access to or
174 the unauthorized modification, disclosure, or destruction of:

2016624er

175 1. Data or information, whether physical or virtual; or

176 2. Information technology resources, which includes:

177 a. Information relating to the security of the agency's
178 technologies, processes, and practices designed to protect
179 networks, computers, data processing software, and data from
180 attack, damage, or unauthorized access; or

181 b. Security information, whether physical or virtual, which
182 relates to the agency's existing or proposed information
183 technology systems.

184 (b) The Legislature finds that it may be valuable, prudent,
185 or critical to a state agency to have an independent entity
186 conduct a risk assessment, an audit, or an evaluation or
187 complete a report of the state agency's information technology
188 program or related systems. Such documents would likely include
189 an analysis of the state agency's current information technology
190 program or systems which could clearly identify vulnerabilities
191 or gaps in current systems or processes and propose
192 recommendations to remedy identified vulnerabilities. The
193 disclosure of such portions of records would jeopardize the
194 information technology security of the state agency, and
195 compromise the integrity and availability of agency data and
196 information technology resources, which would significantly
197 impair the administration of governmental programs. It is
198 necessary that such portions of records be made confidential and
199 exempt from public records requirements in order to protect
200 agency technology systems, resources, and data. The Legislature
201 further finds that this public records exemption shall be given
202 retroactive application because it is remedial in nature.

203 Section 3. This act shall take effect upon becoming a law.