

1 AN ACT concerning State government.

2 **Be it enacted by the People of the State of Illinois,**
3 **represented in the General Assembly:**

4 Section 5. The Department of Innovation and Technology Act
5 is amended by changing Sections 1-5, 1-10, 1-15, and 1-25 as
6 follows:

7 (20 ILCS 1370/1-5)

8 Sec. 1-5. Definitions. In this Act:

9 ~~"Client agency" means each transferring agency, or its~~
10 ~~successor, and any other public agency to which the Department~~
11 ~~provides service to the extent specified in an interagency~~
12 ~~agreement with the public agency.~~

13 "Dedicated unit" means the dedicated bureau, division,
14 office, or other unit within a transferred ~~transferring~~ agency
15 that is responsible for the information technology functions
16 of the transferred ~~transferring~~ agency.

17 "Department" means the Department of Innovation and
18 Technology.

19 "Information technology" means technology,
20 infrastructure, equipment, systems, software, networks, and
21 processes used to create, send, receive, and store electronic
22 or digital information, including, without limitation,
23 computer systems and telecommunication services and systems.

1 "Information technology" shall be construed broadly to
2 incorporate future technologies that change or supplant those
3 in effect as of the effective date of this Act.

4 "Information technology functions" means the development,
5 procurement, installation, retention, maintenance, operation,
6 possession, storage, and related functions of all information
7 technology.

8 "Secretary" means the Secretary of Innovation and
9 Technology.

10 "State agency" means each State agency, department, board,
11 and commission under the jurisdiction of the Governor to which
12 the Department provides services.

13 "Transferred ~~Transferring~~ agency" means the Department on
14 Aging; the Departments of Agriculture, Central Management
15 Services, Children and Family Services, Commerce and Economic
16 Opportunity, Corrections, Employment Security, Financial and
17 Professional Regulation, Healthcare and Family Services, Human
18 Rights, Human Services, Insurance, Juvenile Justice, Labor,
19 Lottery, Military Affairs, Natural Resources, Public Health,
20 Revenue, Transportation, and Veterans' Affairs; the Illinois
21 State Police; the Capital Development Board; the Deaf and Hard
22 of Hearing Commission; the Environmental Protection Agency;
23 the Governor's Office of Management and Budget; the
24 Guardianship and Advocacy Commission; the Abraham Lincoln
25 Presidential Library and Museum; the Illinois Arts Council;
26 the Illinois Council on Developmental Disabilities; the

1 Illinois Emergency Management Agency; the Illinois Gaming
2 Board; the Illinois Liquor Control Commission; the Office of
3 the State Fire Marshal; the Prisoner Review Board; and the
4 Department of Early Childhood.

5 (Source: P.A. 102-376, eff. 1-1-22; 102-538, eff. 8-20-21;
6 102-813, eff. 5-13-22; 102-870, eff. 1-1-23; 103-588, eff.
7 6-5-24.)

8 (20 ILCS 1370/1-10)

9 Sec. 1-10. Transfer of functions. On and after March 25,
10 2016 (the effective date of Executive Order 2016-001):

11 (a) (Blank).

12 (b) (Blank).

13 (c) The personnel of each transferred ~~transferring~~ agency
14 designated by the Governor are transferred to the Department.
15 The status and rights of the employees and the State of
16 Illinois or its transferred ~~transferring~~ agencies under the
17 Personnel Code, the Illinois Public Labor Relations Act, and
18 applicable collective bargaining agreements or under any
19 pension, retirement, or annuity plan shall not be affected by
20 this Act. Under the direction of the Governor, the Secretary,
21 in consultation with the transferred ~~transferring~~ agencies and
22 labor organizations representing the affected employees, shall
23 identify each position and employee who is engaged in the
24 performance of functions transferred to the Department, or
25 engaged in the administration of a law the administration of

1 which is transferred to the Department, to be transferred to
2 the Department. An employee engaged primarily in providing
3 administrative support for information technology functions
4 may be considered engaged in the performance of functions
5 transferred to the Department.

6 (d) All books, records, papers, documents, property (real
7 and personal), contracts, causes of action, and pending
8 business pertaining to the powers, duties, rights, and
9 responsibilities relating to dedicated units and information
10 technology functions transferred under this Act to the
11 Department, including, but not limited to, material in
12 electronic or magnetic format and necessary computer hardware
13 and software, shall be transferred to the Department.

14 (e) All unexpended appropriations and balances and other
15 funds available for use relating to dedicated units and
16 information technology functions transferred under this Act
17 shall be transferred for use by the Department at the
18 direction of the Governor. Unexpended balances so transferred
19 shall be expended only for the purpose for which the
20 appropriations were originally made.

21 (f) The powers, duties, rights, and responsibilities
22 relating to dedicated units and information technology
23 functions transferred by this Act shall be vested in and shall
24 be exercised by the Department.

25 (g) Whenever reports or notices are now required to be
26 made or given or papers or documents furnished or served by any

1 person to or upon each dedicated unit in connection with any of
2 the powers, duties, rights, and responsibilities relating to
3 information technology functions transferred by this Act, the
4 same shall be made, given, furnished, or served in the same
5 manner to or upon the Department.

6 (h) This Act does not affect any act done, ratified, or
7 canceled or any right occurring or established or any action
8 or proceeding had or commenced in an administrative, civil, or
9 criminal cause by each dedicated unit relating to information
10 technology functions before the transfer of responsibilities
11 under this Act; such actions or proceedings may be prosecuted
12 and continued by the Department.

13 (i) (Blank).

14 (j) (Blank).

15 (Source: P.A. 102-376, eff. 1-1-22.)

16 (20 ILCS 1370/1-15)

17 Sec. 1-15. Powers and duties.

18 (a) The head officer of the Department is the Secretary,
19 who shall be the chief information officer for the State and
20 the steward of State data with respect to those transferred
21 agencies under the jurisdiction of the Governor. The Secretary
22 shall be appointed by the Governor, with the advice and
23 consent of the Senate. The Department may employ or retain
24 other persons to assist in the discharge of its functions,
25 subject to the Personnel Code.

1 (b) The Department shall promote best-in-class innovation
2 and technology to transferred ~~client~~ agencies to foster
3 collaboration among ~~client~~ agencies, empower ~~client~~ agencies
4 to provide better service to residents of Illinois, and
5 maximize the value of taxpayer resources. The Department shall
6 be responsible for information technology functions on behalf
7 of transferred ~~client~~ agencies.

8 (c) When requested and when in the best interest of the
9 State, the ~~The~~ Department may ~~shall~~ provide for and assist
10 with ~~coordinate~~ information technology for non-transferred
11 State agencies, ~~and, when requested and when in the best~~
12 ~~interests of the State,~~ for State constitutional offices,
13 other State government entities, units of federal or local
14 governments, and public and not-for-profit institutions of
15 primary, secondary, and higher education, or other parties not
16 associated with State government. The Department shall
17 establish charges for information technology for State
18 agencies, ~~and, when requested,~~ for State constitutional
19 offices, other State government entities, units of federal or
20 local government, and public and not-for-profit institutions
21 of primary, secondary, or higher education and for use by
22 other parties not associated with State government for any
23 services requested or provided. Entities charged for these
24 services shall make payment to the Department. The Department
25 may instruct ~~all~~ State agencies to report their usage of
26 information technology regularly to the Department in the

1 manner the Secretary may prescribe.

2 (d) The Department shall establish principles ~~develop~~ and
3 ~~implement~~ standards for the protection of, ~~policies, and~~
4 ~~procedures to protect the~~ security and interoperability of
5 State data with respect to State ~~those~~ agencies ~~under the~~
6 ~~jurisdiction of the Governor,~~ including in particular data
7 that are confidential, sensitive, or protected from disclosure
8 by privacy or other laws, while recognizing and balancing the
9 need for collaboration and public transparency.

10 (e) The Department shall be responsible for providing the
11 Governor with timely, comprehensive, and meaningful
12 information pertinent to the formulation and execution of
13 fiscal policy. In performing this responsibility, the
14 Department shall have the power to do the following:

15 (1) Control the procurement, retention, installation,
16 maintenance, and operation, as specified by the
17 Department, of information technology equipment used by
18 State ~~client~~ agencies in such a manner as to achieve
19 maximum economy and provide appropriate assistance in the
20 development of information suitable for management
21 analysis.

22 (2) Establish principles and standards for the
23 implementation of information technology-related
24 reporting by State ~~client~~ agencies and priorities for
25 completion of research by those agencies in accordance
26 with the requirements for management analysis specified by

1 the Department. State agencies shall work with the
2 Department to follow the principles and standards
3 developed by the Department.

4 (3) Establish charges for information technology and
5 related services requested by transferred ~~client~~ agencies
6 and rendered by the Department. The Department is likewise
7 empowered to establish prices or charges for all
8 information technology reports purchased by State agencies
9 and governmental entities ~~individuals~~ not connected with
10 State government using the Department's services.

11 (4) Instruct all State ~~client~~ agencies to report
12 regularly to the Department, in the manner the Department
13 may prescribe, their usage of information technology, the
14 cost incurred, the information produced, and the
15 procedures followed in obtaining the information. All
16 State ~~client~~ agencies shall request from the Department
17 assistance and consultation in securing any necessary
18 information technology to support their requirements.

19 (5) Examine the accounts and information
20 technology-related data of any organization, body, or
21 agency receiving appropriations from the General Assembly,
22 except for a State constitutional office, the Office of
23 the Executive Inspector General, or any office of the
24 legislative or judicial branches of State government. For
25 a State constitutional office, the Office of the Executive
26 Inspector General, or any office of the legislative or

1 judicial branches of State government, the Department
2 shall have the power to examine the accounts and
3 information technology-related data of the State
4 constitutional office, the Office of the Executive
5 Inspector General, or any office of the legislative or
6 judicial branches of State government when requested by
7 those offices.

8 (6) Install and operate a modern information
9 technology system for State agencies using equipment
10 adequate to satisfy the requirements for analysis and
11 review as specified by the Department. Expenditures for
12 information technology and related services rendered shall
13 be reimbursed by the recipients. The reimbursement shall
14 be determined by the Department as amounts sufficient to
15 reimburse the Technology Management Revolving Fund for
16 expenditures incurred in rendering the services.

17 (f) In addition to the other powers and duties listed in
18 subsection (e), the Department shall analyze the present and
19 future aims, needs, and requirements of information
20 technology, research, and planning for State agencies ~~in order~~
21 to provide for the formulation of overall policy relative to
22 the use of information technology and related equipment by the
23 State of Illinois. In making this analysis, the Department
24 shall formulate a master plan for information technology,
25 using information technology most advantageously, and advising
26 whether information technology should be leased or purchased

1 by the State. The Department shall prepare and submit interim
2 reports of meaningful developments and proposals for
3 legislation to the Governor on or before January 30 each year.
4 The Department shall engage in a continuing analysis and
5 evaluation of the master plan so developed, and it shall be the
6 responsibility of the Department to recommend from time to
7 time any needed amendments and modifications of any master
8 plan enacted by the General Assembly.

9 (g) The Department may make information technology and the
10 use of information technology available to units of local
11 government, elected State officials, State educational
12 institutions, the judicial branch, the legislative branch, and
13 all other governmental units of the State requesting them. The
14 Department shall establish prices and charges for the
15 information technology so furnished and for the use of the
16 information technology. The prices and charges shall be
17 sufficient to reimburse the cost of furnishing the services
18 and use of information technology.

19 (h) The Department may establish principles and standards
20 to provide consistency in the operation and use of information
21 technology by State agencies. State agencies shall work with
22 the Department to follow the principles and standards
23 developed by the Department.

24 (i) The Department may adopt rules under the Illinois
25 Administrative Procedure Act necessary to carry out its
26 responsibilities under this Act.

1 (Source: P.A. 102-376, eff. 1-1-22.)

2 (20 ILCS 1370/1-25)

3 Sec. 1-25. Charges for services; non-State funding. The
4 Department may establish charges for services rendered by the
5 Department to State ~~client~~ agencies from funds provided
6 directly to the State ~~client~~ agency by appropriation or
7 otherwise. In establishing charges, the Department shall
8 consult with State ~~client~~ agencies to make charges transparent
9 and clear and seek to minimize or avoid charges for costs for
10 which the Department has other funding sources available.

11 State ~~Client~~ agencies shall continue to apply for and
12 otherwise seek federal funds and other capital and operational
13 resources for technology for which the agencies are eligible
14 and, subject to compliance with applicable laws, regulations,
15 and grant terms, make those funds available for use by the
16 Department.

17 (Source: P.A. 102-870, eff. 1-1-23.)

18 (20 ILCS 1370/1-75 rep.)

19 Section 10. The Department of Innovation and Technology
20 Act is amended by repealing Section 1-75.

21 Section 15. The Illinois Information Security Improvement
22 Act is amended by changing Sections 5-5, 5-15, and 5-25 and by
23 adding Section 5-35 as follows:

1 (20 ILCS 1375/5-5)

2 Sec. 5-5. Definitions. As used in this Act:

3 "Critical information system" means any information system
4 (including any telecommunications system) used or operated by
5 a State agency or by a contractor of a State agency or other
6 organization or entity on behalf of a State agency: that
7 contains health insurance information, medical information, or
8 personal information as defined in the Personal Information
9 Protection Act; where the unauthorized disclosure,
10 modification, destruction of information in the information
11 system could be expected to have a serious, severe, or
12 catastrophic adverse effect on State agency operations,
13 assets, or individuals; or where the disruption of access to
14 or use of the information or information system could be
15 expected to have a serious, severe, or catastrophic adverse
16 effect on State operations, assets, or individuals.

17 "Department" means the Department of Innovation and
18 Technology.

19 "Information security" means protecting information and
20 information systems from unauthorized access, use, disclosure,
21 disruption, modification, or destruction in order to provide:
22 integrity, which means guarding against improper information
23 modification or destruction, and includes ensuring information
24 non-repudiation and authenticity; confidentiality, which means
25 preserving authorized restrictions on access and disclosure,

1 including means for protecting personal privacy and
2 proprietary information; and availability, which means
3 ensuring timely and reliable access to and use of information.

4 "Incident" means an occurrence that: actually or
5 imminently jeopardizes, without lawful authority, the
6 confidentiality, integrity, or availability of information or
7 an information system; or constitutes a violation or imminent
8 threat of violation of law, security policies, security
9 procedures, or acceptable use policies or standard security
10 practices.

11 "Information system" means a discrete set of information
12 resources organized for the collection, processing,
13 maintenance, use, sharing, dissemination, or disposition of
14 information created or maintained by or for the State of
15 Illinois.

16 "Office" means the Office of the Statewide Chief
17 Information Security Officer.

18 "Secretary" means the Secretary of Innovation and
19 Technology.

20 "Security controls" means the management, operational, and
21 technical controls (including safeguards and countermeasures)
22 for an information system that protect the confidentiality,
23 integrity, and availability of the system and its information.

24 "State agency" means any State agency, department, board,
25 and commission under the jurisdiction of the Governor to which
26 the Department provides services.

1 (Source: P.A. 100-611, eff. 7-20-18.)

2 (20 ILCS 1375/5-15)

3 Sec. 5-15. Office of the Statewide Chief Information
4 Security Officer.

5 (a) The Office of the Statewide Chief Information Security
6 Officer is established within the Department of Innovation and
7 Technology. The Office is directly subordinate to the
8 Secretary of Innovation and Technology.

9 (b) The Office shall:

10 (1) serve as the strategic planning, facilitation, and
11 coordination office for information technology security in
12 this State and as the lead and central coordinating entity
13 to guide and oversee the information security functions of
14 State agencies;

15 (2) provide information security services to support
16 the secure delivery of State agency services that utilize
17 information systems and to assist State agencies with
18 fulfilling their responsibilities under this Act;

19 (3) conduct information and cybersecurity strategic,
20 operational, and resource planning and facilitating an
21 effective enterprise information security architecture
22 capable of protecting the State;

23 (4) identify information security risks to each State
24 agency, to third-party providers, and to key supply chain
25 partners, including an assessment of the extent to which

1 information resources or processes are vulnerable to
2 unauthorized access or harm, including the extent to which
3 the State agency's or contractor's electronically stored
4 information is vulnerable to unauthorized access, use,
5 disclosure, disruption, modification, or destruction, and
6 recommend risk mitigation strategies, methods, and
7 procedures to reduce those risks. These assessments shall
8 also include, but not be limited to, assessments of
9 information systems, computers, printers, software,
10 computer networks, interfaces to computer systems, mobile
11 and peripheral device sensors, and other devices or
12 systems which access the State's network, computer
13 software, and information processing or operational
14 procedures of the State agency or of a contractor of the
15 State agency.

16 (5) manage the response to information security and
17 information security incidents involving State agency
18 ~~State of Illinois~~ information systems and ensure the
19 completeness of information system security plans for
20 critical information systems;

21 (6) conduct pre-deployment information security
22 assessments for critical information systems and submit
23 findings and recommendations to the Secretary and State
24 agency heads;

25 (7) develop and conduct targeted operational
26 evaluations, including threat and vulnerability

1 assessments on State agency information systems;

2 (8) monitor and report ~~compliance of each~~ State
3 agency's compliance ~~agency~~ with State information security
4 policies, standards, and procedures;

5 (9) coordinate statewide information security
6 awareness and training programs; and

7 (10) develop and execute other strategies as necessary
8 to protect State agency's ~~this State's~~ information
9 technology infrastructure and the data stored on or
10 transmitted by such infrastructure.

11 (c) The Office may temporarily suspend operation of an
12 information system or information technology infrastructure
13 that is owned, leased, outsourced, or shared by one or more
14 State agencies ~~in order~~ to isolate the source of, or stop the
15 spread of, an information security breach or other similar
16 information security incident. State agencies shall comply
17 with directives to temporarily discontinue or suspend
18 operations of information systems or information technology
19 infrastructure.

20 (Source: P.A. 100-611, eff. 7-20-18.)

21 (20 ILCS 1375/5-25)

22 Sec. 5-25. Responsibilities.

23 (a) The Secretary shall:

24 (1) appoint a Statewide Chief Information Security
25 Officer pursuant to Section 5-20;

1 (2) provide the Office with the staffing and resources
2 deemed necessary by the Secretary to fulfill the
3 responsibilities of the Office;

4 (3) oversee statewide information security policies
5 and practices for State agencies, including:

6 (A) directing and overseeing the development,
7 implementation, and communication of statewide
8 information security policies, standards, and
9 guidelines;

10 (B) overseeing the education of ~~State~~ agency
11 personnel regarding the requirement to identify and
12 provide information security protections commensurate
13 with the risk and magnitude of the harm resulting from
14 the unauthorized access, use, disclosure, disruption,
15 modification, or destruction of information in a
16 critical information system;

17 (C) overseeing the development and implementation
18 of a statewide information security risk management
19 program;

20 (D) overseeing ~~State~~ agency compliance with the
21 requirements of this Section;

22 (E) coordinating Information Security policies and
23 practices with related information and personnel
24 resources management policies and procedures; and

25 (F) providing an effective and efficient process
26 to assist ~~State~~ agencies with complying with the

1 requirements of this Act; and

2 (4) subject to appropriation, establish a
3 cybersecurity liaison program to advise and assist units
4 of local government in identifying cyber threats,
5 performing risk assessments, sharing best practices, and
6 responding to cyber incidents.

7 (b) The Statewide Chief Information Security Officer
8 shall:

9 (1) serve as the head of the Office and ensure the
10 execution of the responsibilities of the Office as set
11 forth in subsection (c) of Section 5-15, the Statewide
12 Chief Information Security Officer shall also oversee
13 State agency personnel with significant responsibilities
14 for information security and ensure a competent workforce
15 that keeps pace with the changing information security
16 environment;

17 (2) develop and recommend information security
18 policies, standards, procedures, and guidelines to the
19 Secretary for statewide adoption and monitor compliance
20 with these policies, standards, guidelines, and procedures
21 through periodic testing;

22 (3) develop and maintain risk-based, cost-effective
23 information security programs and control techniques to
24 address all applicable security and compliance
25 requirements throughout the life cycle of State agency
26 information systems;

1 (4) establish the procedures, processes, and
2 technologies for State agencies to rapidly and effectively
3 identify threats, risks, and vulnerabilities to State
4 information systems, and ensure the prioritization of the
5 remediation of vulnerabilities that pose risk to the
6 State;

7 (5) develop and implement capabilities and procedures
8 for detecting, reporting, and responding to information
9 security incidents;

10 (6) establish and direct a statewide information
11 security risk management program to identify information
12 security risks in State agencies and deploy risk
13 mitigation strategies, processes, and procedures;

14 (7) establish the State's capability to sufficiently
15 protect the security of data through effective information
16 system security planning, secure system development,
17 acquisition, and deployment, the application of protective
18 technologies and information system certification,
19 accreditation, and assessments;

20 (8) ensure that State agency personnel, including
21 contractors, are appropriately screened and receive
22 information security awareness training;

23 (9) convene meetings with State agency heads and other
24 State officials to help ensure:

25 (A) the ongoing communication of risk and risk
26 reduction strategies,

1 (B) effective implementation of information
2 security policies and practices, and

3 (C) the incorporation of and compliance with
4 information security policies, standards, and
5 guidelines into the policies and procedures of the
6 State agencies;

7 (10) provide operational and technical assistance to
8 State agencies in implementing policies, principles,
9 standards, and guidelines on information security,
10 including implementation of standards promulgated under
11 subparagraph (A) of paragraph (3) of subsection (a) of
12 this Section, and provide assistance and effective and
13 efficient means for State agencies to comply with the
14 State agency requirements under this Act;

15 (11) in coordination and consultation with the
16 Secretary and the Governor's Office of Management and
17 Budget, review State agency budget requests related to
18 Information Security systems and provide recommendations
19 to the Governor's Office of Management and Budget;

20 (12) ensure the preparation and maintenance of plans
21 and procedures to provide cyber resilience and continuity
22 of operations for critical information systems that
23 support the operations of the State; and

24 (13) take such other actions as the Secretary may
25 direct.

26 (Source: P.A. 101-81, eff. 7-12-19; 102-753, eff. 1-1-23.)

1 (20 ILCS 1375/5-35 new)

2 Sec. 5-35. Local government cybersecurity designee. The
3 principal executive officer, or his or her designee, of each
4 municipality with a population of 35,000 or greater and of
5 each county shall designate a local official or employee as
6 the primary point of contact for local cybersecurity issues.
7 Each jurisdiction must provide the name and contact
8 information of the cybersecurity designee to the Statewide
9 Chief Information Security Officer and update the information
10 as necessary.