SECTION 16

PLANNING AND MANAGEMENT OF INFORMATION TECHNOLOGY

16.02 CYBERSECURITY POLICIES

AUTHORITY: *FINANCIAL ADMINISTRATION ACT*

ADMINISTRATION: TREASURY BOARD SECRETARIAT
IT SHARED SERVICES

EFFECTIVE DATE: JUNE 2024

16.02 CYBERSECURITY POLICIES

(1) PURPOSE

The purpose of this section of the Policy Manual is to set out Government's policy for the secure processing and storage of sensitive government information on Information Technology delivery systems.

(2) APPLICATION

The application of this policy is referenced to the schedules of the *Financial Administration Act* (FAA) and applies as follows:

- Schedule "A" - Departments except the Legislative Assembly
- Schedule "B" - Crown corporations
- Schedule "C" - Education Authorities
- Schedule "D" - Commissions

except to the extent that their enabling legislation may incorporate alternate requirements such as Ministerial or Board Authority. In the event that a policy developed by Ministerial or Board Authorities differs from Treasury Board policy and that entity is accessing Government IT services, Treasury Board Policy will prevail.

While this policy **does not apply** to the Legislative Assembly or to Reporting Entities subject to alternate legislation, **the spirit and intent** of the policy should serve as a **guideline** for these entities in developing their own policies. Reporting Entities that develop policies differing from Treasury Board require approval of Treasury Board.

(3) DEFINITIONS

For the purpose of this policy, the following definitions will apply:

(a) **"Cybersecurity"** refers to the body of technologies, processes and practices designed to protect networks, devices, applications and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

(b) "**Departments**" mean departments, Crown corporations, agencies, boards, authorities, commissions and other organizations using Government IT services.

(c) **"Emergency Security Directives"** provide direction by the Corporate Information Security Officer, on behalf of the Secretary to the Treasury Board and after authorization is provided by the Clerk of Executive Council, in the event that an action needs to be taken immediately in order to protect the Government information management and information technology security, before a new policy instrument has been finalized.

(d) "**Information Technology (IT)**" means the application of hardware, software, consultation and technical skills to support program delivery and administration and to meet fiscal goals.

(e) **"Non-Compliance Security Directives"** provide direction by the Corporate Information Security Officer, after authorization is provided by the Clerk of Executive Council, when it is necessary to escalate the communication of policy non-compliance, when that non-compliance has a Government information management and information technology cybersecurity impact.

(f) **"Government Information Security Framework (GISF)"** establishes a framework for cybersecurity policies for the Government of Prince Edward Island and any Entities receiving services from Information Technology Shared Services (ITSS). Due to the integrated nature of information management and information technology throughout Government, the objective of the GISF is to outline foundational cybersecurity policy requirements to ensure a consistent level of protection for all users of Government's technology. Policy instruments will be developed in support of the GISF to provide additional direction on risk management and cybersecurity.

(g) **"Exception to the GISF"** means approval to waive or suspend an element of one of the policies contained in the Government Information Security Framework. The procedure for requesting an exception is found within the GISF itself.

(4) POLICY

All Government information and technology systems are to be protected from unauthorized access, disclosure, removal, modification and/or interruption. The GISF will outline the major areas where cybersecurity considerations must be addressed, supported by standards, procedures and guidelines as the minimum requirements for providing a secure environment for developing, implementing, and supporting information technology infrastructure and systems.

The GISF will include, but is not limited to, the following areas:

- Asset Management;
- Employee Cybersecurity;
- Physical and Environmental Cybersecurity;
- Communications and Operations Management;
- Access Control;
- Systems Acquisition, Development and Maintenance;
- Cybersecurity Incident Management;
- Business Continuity Management;
- Compliance;
- Data and Information Classification;
- Digital Identity; and
- Cloud.

(5) PROCEDURE

(a) The Secretary to Treasury Board

The Secretary to Treasury Board is responsible for developing, approving and maintaining the GISF and all policy instruments developed in the support of the GISF.

(b) Digital and Information Advisory Council (DIAC)

DIAC will provide advice and recommendations to the Secretary to Treasury Board, when required by the Secretary to Treasury Board

(c) Treasury Board Secretariat, Information Technology Shared Services

ITSS will:

(i) identify, draft and review policy instruments in support of the GISF;

(ii) perform an annual review of the GISF and cybersecurity procedures and provide a report on the state of IT security in Government to the Secretary to Treasury Board;

(iii) issue Non-Compliance Security Directives, when necessary and after authorization is provided by the Clerk of Executive Council, to escalate the communication of policy non-compliance when that non-compliance has a Government information management and information technology security impact;

(iv) issue Emergency Security Directives, after authorization is provided by the Clerk of Executive Council, in the event that an action needs to be taken immediately in order to protect the Government information management and information technology security; and

(v) review requests for exemption by Departments prior to a Department implementing any changes that would affect the level of cybersecurity required by the GISF.

(d) Departments

Each department will:

(i) comply with the GISF and any associated instruments;

(ii) provide timely response to address Non-Compliance Security Directives and confirm the response was deemed acceptable to the Secretary to Treasury Board;

(iii) immediately respond and address Emergency Security Directives in a manner deemed acceptable to the Secretary to Treasury Board;

(iv) work with Security Services to ensure implementation of the GISF; and

(v) through the Deputy Head, provide written requests for exceptions to the GISF to Security Services.

(6) OTHER DOCUMENTS PERTAINING TO INFORMATION TECHNOLOGY CYBERSECURITY

Supporting documents related to cybersecurity will be maintained by ITSS and made available internally to those who are provided access to Government systems.

(7) INTERPRETATION

In cases where an interpretation is required, such should be referred to the Secretary to Treasury Board or their delegated officer who will make the interpretation or refer the matter to Treasury Board, if a Treasury Board decision is deemed necessary.