KINGSTON POLICE SERVICE BOARD

Information Technology and Information Security Policy (AI-020)

Adopted: Sept. 4/26
Reviewed:
Revised:

Expires: Indefinite

Rescinds:

Legislation: Community Safety and Policing Act, 2019.

1. **Policy Statement**

The Kingston Police Service Board (the Board) recognizes the importance of maintaining a secure and reliable information technology environment to support the effective delivery of policing services and protect the confidentiality, integrity, and availability of police information and information systems. The Board is committed to ensuring that access to police databases and information systems is appropriately authorized, controlled, monitored, and protected against unauthorized access, misuse, and security threats.

2. **Board Policy**

It is the policy of the Kingston Police Service Board, with respect to information technology and information security, that the Chief of Police will:

a) Establish and maintain information technology and information security procedures appropriate to the Service's operational and organizational requirements and applicable legal and regulatory obligations.

b) Ensure that access to police databases and information systems is:

i. Authorized based on a member's role, responsibilities, and current duties;

ii. Limited in accordance with the principle of least privilege;

iii. Appropriately managed when a member's role, responsibilities, or duties change; and

iv. Revoked or otherwise appropriately restricted when access is no longer required.

c) Ensure that appropriate controls are established for the authorization, assignment, review, modification, and removal of access permissions to police databases and information systems.

d) Ensure that appropriate controls are established for privileged or elevated access to police databases and information systems.

e) Ensure that police databases and information systems are appropriately monitored to identify unauthorized or inappropriate access and activity.

f) Ensure that monitoring mechanisms support both:

i. Proactive identification of potential misuse and early warning signs of unauthorized or inappropriate activity; and

ii. Reactive review of access and system activity where potential misuse, unauthorized access, or a security incident is suspected or identified.

g) Ensure that confidential, sensitive, and police information is appropriately protected against unauthorized access, use, disclosure, loss, or destruction.

h) Ensure that safeguards are established to protect the Service's information technology environment against cybersecurity threats and unauthorized access.

i) Ensure that members are provided with appropriate information, training, and direction regarding their responsibilities for information security, including the appropriate use and protection of information technology resources and police information.

j) Ensure that procedures are established for members to promptly report suspected or confirmed information security incidents, including unauthorized access to or use of police databases and information systems.

k) Ensure that significant information security incidents, systemic concerns, or material risks are reported to the Board.

l) Ensure that the Service's information technology and information security framework is periodically reviewed and updated to address identified risks, changes to the Service's information technology environment, applicable legislative and regulatory requirements, and recognized practices.

"original signed by Chair"	"original signed by Board Administrator"
Chair	Board Administrator