**OFFICE OF THE CHIEF OF POLICE**

**ADMINISTRATIVE ORDER NO.** 7 July 20, 2023

**SUBJECT:** **PROHIBITING ACCESS TO PERSONAL EMAIL ACCOUNTS ON DEPARTMENT WORKSTATIONS – ESTABLISHED**

**PURPOSE:** The purpose of this Order is to establish a policy prohibiting Department personnel from accessing their personal email accounts on Department workstations. The steady increase in the use of phishing emails to compromise organizations world-wide has forced the Department to reevaluate, "acceptable use." Department employees are reminded that the use of the internet or email on a Department workstation shall be restricted to, "official Department business."

**PROCEDURE:** Department Manual Section 3/788.42, *Prohibiting Access to Personal Email Accounts on Department Workstations*, has been established and is attached.

**AMENDMENT:** This Order adds Section 3/788.42 to the Department Manual.

**AUDIT RESPONSIBILITY:** The Commanding Officer, Audit Division, shall review this directive and determine whether an audit or inspection shall be conducted in accordance with Department Manual Section 0/080.30.

MICHEL R. MOORE
Chief of Police

Attachment

DISTRIBUTION "D"

***788.42 PROHIBITING ACCESS TO PERSONAL EMAIL ACCOUNTS ON DEPARTMENT WORKSTATIONS.*** *Due to phishing being the number one method of initial compromise in cyberattacks, Department workstations (any desktop PC joined to the Department domain) shall only be utilized to access Department email accounts issued by Information Technology Division (ITD). "Phishing" is the use of electronic mail to acquire unauthorized access to sensitive information or to infect a workstation with malicious software.*

> ***Note:*** *The provisions of this Section apply to all Department personnel including sworn, civilian, volunteers, reserves, and any third-party vendors contracted by the Department.*

***Employee's Responsibilities.*** *Employees are prohibited from accessing any email accounts not issued or authorized by ITD on any Department workstation.*

> ***Exemptions:*** *Employees who require access to a non-ITD issued or authorized email account on a Department workstation to conduct Department business shall complete an Intradepartmental Correspondence, Form 15.02.00 (15.02), to ITD.*

*All requests for exemptions shall be approved by each respective requesting Area/division Commanding Officer (CO) and ITD prior to the employee gaining access.*

***Area/Division Commanding Officer's Responsibilities.*** *Area/division COs shall approve or deny all requests for access to non-ITD issued or authorized email accounts from a Department workstation prior to submitting the 15.02 to ITD.*

***Information Technology Division's Responsibilities.*** *Information Technology Division shall restrict access to non-ITD issued or authorized email accounts on any Department workstation and shall provide final approval for exemption. Information Technology Division shall also conduct periodic exemption audits to ensure exemptions remain current and applicable.*