	POLICY & PROCEDURE	SERIES # **559**	PAGE 1 OF 3
	SUBJECT **CYBER SECURITY AND INFORMATION SECURITY PRACTICES**		EFFECTIVE DATE **02/05/2019**
			OVERSIGHT **Planning, Research and Analysis**
	DISTRIBUTION **ALL MANUALS**	AMENDS/SUPERSEDES/CANCELS P&P # NEW POLICY	

I. PURPOSE:

The purpose of this policy is to establish effective Cyber Security and Information Security practices for employees of the Hampton Police Division as well as response protocols for Cyber Security Incidents.

II. POLICY:

It is the policy of Hampton Police Division that all employees will utilize practices that promote the safeguarding of all City of Hampton Information Technology Assets. This will be promoted through training that will be required of all Hampton Police Division Employees to complete.

III. DEFINITIONS:

City of Hampton Information Technology Asset: A City of Hampton Technology Asset is defined as any computer, mobile device, server, software application, network device or database that belongs to or is licensed to the City of Hampton.

Cyber Incident Investigation Liaison: A designee that is a member of the Hampton Police Division who is responsible for investigating any Cyber Security Incidents that have occurred within the City of Hampton Network. Investigations will be conducted with the cooperation of both Hampton Police Division Information Technology Employees and City of Hampton Information Technology Employees. This liaison will be selected by the Chief of Police or his designee.

Cyber Security Incident: Any incident, whether unintentional or with malicious intent, in which an actor is able to or attempts to gain unauthorized access to a City of Hampton Information Technology Asset.

Cyber Security: Techniques that are utilized to safeguard computers, networks, software applications and data from unauthorized access or intrusive activities.

Information: Consists of any data or knowledge that is collected, stored, processed, managed or transferred for any purpose.

Malware: Software that is designed to cause damage to a computer(s) or a computer network.

Network Intrusion: Any unauthorized activity that occurs on a computer network.

Phishing: The act of sending emails that are purported to be from legitimate organizations or individuals with the purpose of inducing the recipient into sharing personal information (e.g. passwords and financial information).

IV. PROCEDURE:

A. Upon discovering that a Cyber Security Incident has occurred which involves a City of Hampton Information Technology Asset, it will be the responsibility of the employee to notify their supervisor to ensure that the liaison is notified within 24 hours of the incident reporting. If it is an incident involving an active Network Intrusion of a City of Hampton Asset, the liaison should be immediately notified.

B. In an effort to provide adequate triage measures for Cyber Security Incidents, the Hampton Police Division Cyber Investigation Liaison will be notified for the following situations:

a. In the event that any employee executes a phishing link that is contained within any email message received in their City of Hampton Email Account.

b. In the event that any employee executes a phishing link that is contained within their personal email account while connected to the City of Hampton Network.

c. For any instance in which an email that is registered to the City of Hampton Domain is compromised (e.g. account takeover).

d. In the event that any unauthorized access is made to the City of Hampton Network, any database that contains information that

belongs to the City of Hampton, or any software application that is owned by or licensed to the Hampton Police Division.

C. In order to create an environment that is resistant to malicious activity, the following procedures will be followed:

a. Any and all City of Hampton Information Technology assets contained within the City of Hampton Network must not utilize default credentials for the purpose of authentication.

b. Plain text passwords that belong to any Information Systems that are owned or licensed to the City of Hampton will not be transmitted through the City of Hampton Email Domain.

c. Plain text passwords that belong to any Information Systems that are owned or licensed to the City of Hampton will not be transmitted through any personal email account.

d. Currently utilized passwords should never be shared, offered or requested via email, text, telephone call or any other data transmission method for any City of Hampton Information Technology Asset.

e. In the instance that a password must be reset, the password reset information should be sent to a Hampton Police Division Issued Cell phone via text message that is properly locked per Hampton Police Division Policy. Upon sending and receiving the text message containing the reset information, the message should be deleted by the sender and the recipient.

f. Usernames and passwords should not be written on any physical document that is not stored in a secured location or any electronic document that lacks encryption.