Policy Name:	**INFORMATION TECHNOLOGY (IT) SECURITY**		
Policy #:	AD 9.19	**Last Updated:**	2022-11-30
Issued By:	SUPPORT SERVICES BUREAU	**Approved By:**	SURREY POLICE BOARD
		Review Frequency:	AS REQUIRED

RELATED POLICIES

AD 9.1 *Authorized Use of Computing Environment and Electronic Communications*

AD 9.14 *Records Administration & Retention*

AD 9.17 *Social Media*

AD 9.18 *Security and Confidentiality of Records and Information*

1. PURPOSE

1.1. This policy applies to all equipment and systems that are owned or leased by SPS, and to personal computing equipment that is used, with authorization, for SPS purposes, regardless of physical location.

1.2. This policy is consistent with the *Police Act*, BC *Provincial Policing Standards*, BC *Human Rights Code*, provincial privacy legislation, and related SPS policies.

1.3. The purpose of this policy to is outline security protocols all Users are expected to follow to protect the integrity of SPS solutions and the data that resides on them.

2. SCOPE

2.1. This policy applies to all SPS Employees, and includes Contractors, Practicum Students or Volunteers responsible for ensuring that persons who are granted access to SPS digital and technological resources have read and agree to abide by this policy.

3. POLICY

3.1. SPS recognizes that email, Internet access, and Information Technology (IT) are useful and necessary services that enhance ability to communicate with others, effectively share data, and provides

improved service to the public. The purpose of this policy sets appropriate standards for using IT resources.

3.2. The information transmitted on the Internet or stored on servers accessible via the Internet is generally an insecure environment and content may be viewed by non-intended audiences. Users must not knowingly access sites that may bring SPS into disrepute. This applies to email as email may be intercepted by non-intended recipients and/or forwarded beyond the control of the sender. SPS has a responsibility to ensure email procedures are adhered to (see AD 9.1 *Authorized Use of Computing Environment and Electronic Communications;* AD 9.17 *Social Media*).

4. PROCEDURE

Review and Audit

4.1. The Information Technology Unit (ITU) will routinely analyze network traffic for trends or anomalies.

i. Breaches of policy and/or evidence of misconduct may be found during these searches intended to protect the SPS network.
ii. Alleged breaches of policy or misuse of SPS email or the Internet may result in a labour process investigation, an investigation under the *Police Act*, and/or *Criminal Code*.

4.2. SPS may access, audit, monitor, inspect, copy, store, and review SPS IT resources, without prior notice, upon receiving a complaint of misconduct regarding inappropriate email content, text or attachments, Internet usage, or the inappropriate release of Classified or Protected information.

i. When such and audit occurs, a log detailing all access will be maintained by the investigator conducting the audit.
ii. During an audit or an investigation, if there is uncertainty about the appropriateness of the content in an email or on the network, consultation may occur with internal stakeholders and experts in this field. This may include:
    a) the Inspector i/c Special Investigation Section;
    b) the Inspector i/c Employee Services Section;
    c) a union representative; or
    d) any other expert who may provide clarity around the appropriateness of such material.

Security Access – Internet and Email

4.3. Users who access Internet URLs may be required to explain why they have accessed a particular site.

4.4. ITU may revoke or restrict Internet access to any or all Users for valid technical reasons (e.g., bandwidth restrictions, virus/worm attack, disaster or emergency response, or other technical requirements).

4.5. Users accessing or disseminating information on the Internet must ensure that such information is in compliance with SPS policies and applicable federal and provincial law (see AD 5.7 *Human Rights and Respectful Workplace*; AD 9.1 *Authorized Use of Computing Environment and Electronic Communications*; AD 9.17 *Social Media*).

4.6. Users must comply with all applicable laws and regulations and respect the legal protection provided by copyright and licenses with respect to programs, software applications and data.

4.7. Third parties may be able to gain access to data, records or communications transmitted by email, through an FOI request, a subpoena or summons in a court of law, internal usage monitoring, or interception on the Internet. As a result, Users must consider what information they are transmitting by email. In addition, Internet and email users must not disclose User identifications, passwords, or any other non-public identifiers of anyone, including Employee information, or any detail of SPS's security measures.

Passwords

4.8. SPS may require the use of certificates, two factor authentication, or other security mechanisms for Users to access SPS Computing Environment and Electronic Communications.

4.9.Users must protect all passwords.

i. User Passwords for computer workstation logins must be kept confidential;
ii. Passwords must not be posted in or around the User's workstation; and
iii. Users must not share identification or password codes for SPS digital equipment unless using a designated shared workstation that requires a shared password (e.g., Intellibook).

4.10. Users must not attempt to obscure the origin or destination of any transmission, or download material under an assumed Internet address, except for investigative purposes and with the written approval of an ITU Manager.

4.11. Users must ensure computer equipment is locked or logged off when absent from the workstation. Any person accessing another User's workstation or electronic device without authorization violates this policy and may be subject to discipline under the *Police Act* or labour process.

4.12. SPS recognizes that Employees, on occasion, may be working remotely and may have custody or issued equipment to facilitate computer access. Users working remotely are responsible for the security of SPS equipment, digital resources, and data (see AD 9.1 *Authorized Use of Computing Environment and Electronic Communications*).

Mobile Devices - Guidelines

4.13. The following guidelines apply to the use of SPS mobile devices (i.e., cellphones, laptops, and mobile workstations):

i. Loss, theft, or other security incidents related to an SPS-provided mobile device must be reported promptly to the SPS IT ServiceDesk and the User's Supervisor.
ii. Protected "B" and Protected "C" data must not be stored on SPS mobile devices unless necessary. If Protected "B" and Protected "C" data is stored on a mobile device, it must be appropriately secured and comply with the policy.
iii. Users are not to store SPS data on personal mobile equipment.

IT Security Incidents

4.14. An IT Security Incident can take one of two forms:

i. Electronic: This type of incident can range from an attacker or User accessing the network for unauthorized/malicious purposes, to a virus outbreak, to a suspected Trojan or malware infection.
ii. Physical: A physical IT Security Incident involves the loss or theft of a laptop, mobile device, removable media, or failure to protect Protected "B" or Protected "C" data.

4.15. When an IT Security Incident is suspected, SPS's goal is to recover the data as quickly as possible, limit the damage done, secure the network, and preserve evidence of the incident. The following steps must be taken:

4.16. When an IT Security Incident is suspected, SPS's goal is to secure the network, limit the damage done, recover the data as quickly as possible, and preserve evidence of the incident. If Users suspect their device or email may have been compromised the following steps MUST be taken:

i. Immediately call the SPS IT ServiceDesk to speak to an agent and report the incident. If the incident occurs outside of regular hours their call will be routed to an on-call IT analyst. Security incidents are time critical it is essential Users speak to an IT representative in person to ensure awareness. IT representative will gather critical information and escalate to the IT Cyber Security team as required.
ii. Working with the affected User, IT Staff will follow defined Incident Response steps to protect assets, data and preserve evidence, this may include:
    a. remove the compromised device from the network by unplugging or disabling network connection. Do not power down the machine;
    b. disable the compromised account(s) as appropriate;
    c. physically secure the compromised system;
    d. create a detailed event log documenting each step taken during this process;
    e. determine how the attacker gained access and disable this access;
    f. deliver the device to IT or make it available for pick up;
    g. take actions, as possible, to ensure that the vulnerability (or similar vulnerabilities) will not reappear; and
    h. perform a vulnerability assessment to identify any vulnerabilities before they can be exploited.
iii. IT Cyber Security team will escalate confirmed breaches and/or high-risk incidents to the IT Manager and the Information & Privacy Unit Manager.
iv. immediately report the incident to the User's Supervisor and ITU Supervisor.

Account Termination/ Suspension

4.17. Employee Services Section and Human Resources Section must inform the IT ServiceDesk in the event of a staffing change (e.g., Employee transfer, employment termination, employment suspension, extended leave, etc.).

APPENDIX A: DEFINITIONS

"Classified/Protected Data" means data that is classified as:

i. Protected A – Low Sensitivity: information that should not be disclosed to the public without authorization and could reasonably be expected to cause injury or harm.
ii. Protected B – Particularly Sensitive: information that could cause severe injury or damage to the people or group involved if it was disclosed.
iii. Protected C – Extremely Sensitive: information that, if compromised, could reasonably be expected to cause extremely grave injury, at less than the national interest level.

"Computing environment" means any electronic information, information system, application, device (including PCs, laptops, mobile devices, and telephones) or other computing technology that is connected to SPS's IT systems (including cloud-based services and mobile services).

"Contractor" means a person or persons who have access to SPS premises or Electronic Communications System, as defined in this policy, for the purpose of providing services or supplies to SPS on a contractual basis.

"Electronic Communications" means any form of digital communications including, but not limited to, email, text/short message service, instant messaging, online chat, social media posts/tweets, blogs, online video/audio posts, telephonic, faxing, and audio/video conferencing.

"Electronic Communications System" means the technology on which the electronic communications occurs.

"Encryption" means the process of encoding data with an algorithm so that it is unintelligible without the key used to protect data during transmission or while stored.

"Employee" means any employee of SPS (including sworn Members and civilian staff).

"Inappropriate material" means materials including, but is not limited to, any material that is pornographic, sexual, or erotic, obscene, lewd, offensive or harassing, threatening, defamatory, racially offensive, promotes violence, hatred, abuse or neglect, or any material which can be reasonably interpreted as offensive or contravenes the BC *Human Rights Code*, *Criminal Code* or any other federal and provincial laws. This includes any material that may bring the reputation of SPS into disrepute.

"Internet" (World Wide Web or www) means a series of interconnected worldwide computer networks, which are in turn, connected to conforming www sites that offer website information/services or offer email services.

"IT Security Incident" means an electronic incident such as an attacker or User accessing the network for unauthorized/malicious purposes (e.g., malware attack) or a physical IT Security Incident, (e.g., the loss or theft of a laptop, mobile device, Smartphone, tablet, failure to protect Classified/Protected data, etc).

“Malware” or "malicious software" means software application designed with malicious intent. Viruses and Trojans are common examples of malware.

“Member” means a sworn Police Officer appointed by the Surrey Police Board.

“Mobile Device” means a portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

“PDA” means Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar, and notes.

“Practicum Students” mean students of a program at a recognized education institution who are engaged at a SPS premises for study, research, work experience, etc.

"Sensitive Information" means personal, confidential, or protected information where the release is unauthorized, including any information which is reasonably likely to be withheld from access under the *Freedom of Information and Protection of Privacy Act* (FOIPPA).

“Smartphone” means a mobile telephone that offers additional applications, such as PDA functions and email.

“Social media” means websites and online applications that allow people and organizations to create, share, and exchange content or to participate in social networking.

“SPS premises” includes, but is not limited to, any property permanently or temporarily under the jurisdiction of SPS, including land, building, job sites, facilities, parking lots, equipment, vehicles, whether owned, leased or used by SPS and wherever located. The work site of a seconded employee is considered an extension of SPS workplace, and therefore SPS premises.

“SPS property” means all assets of SPS, whether temporary, permanent, owned, leased or otherwise acquired, including real, personal or intellectual property, vehicles, chattels, materials, equipment and supplies.

“Supervisor” means a Team Leader, Manager, Staff Sergeant, Sergeant, Inspector, Superintendent, Deputy Chief Constable, Chief Constable, and any other person acting in a supervisory capacity who is accountable for a particular area or shift on behalf of SPS.

“Trojan” or "Trojan Horse" means an application that is disguised as something innocuous or legitimate but harbors a malicious payload. Trojans can be used to covertly and remotely gain access to a computer, log keystrokes, or perform other malicious or destructive acts.

"User" means any person authorized to access SPS email or the Internet, including permanent, temporary, and limited term Employees, Contractors, Volunteers, Practicum Students.

“Virus” or "Computer Virus" means replicating application that attaches itself to other data, infecting files similar to how a virus infects cells. Viruses can be spread through email or via network-connected computers and file systems.

“Volunteer” means a person serving SPS who is not an employee, as defined in this policy, and includes those individuals serving on any board(s), commission(s) or committee(s) established by SPS.

“WEP” means Wired Equivalency Privacy. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. WEP can be cryptographically broken with relative ease.

“WPA” means WIFI Protected Access. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.

APPENDIX B: REFERENCES

BC *Human Rights Code*, R.S.B.C. 1996, c. 210

BC *Police Act*, R.S.B.C. 1996, c. 367