SUBJECT ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES	POLICY NUMBER 8.03	
POLICY MAINTENANCE ADMINISTRATOR: Chief, Bureau of Personnel Services and Chief Information Officer		
PURPOSE/SCOPE: To establish policy and procedures for the use of department Information Technology (IT) resources.		

I. AUTHORITY

Chapter 119, Florida Statutes, Public Records.

Section 281.301, Florida Statutes, Security systems; records and meetings exempt from public access or disclosure.

Section 282.318, Florida Statutes, Security of data and information technology.

Chapter 815, Florida Statutes, Computer-Related Crimes.

Chapter 60L-36, Florida Administrative Code, Conduct of Employees.

Chapter 74-2, Florida Administrative Code, Information Technology Security.

Governor's Executive Order 11-03 and Code of Ethics, effective January 4, 2011

II. RELATED POLICIES

MP 3.06, Disciplinary Process

MP 3.08, Ethics and Personal Responsibility

MP 3.12, Department Fraud

MP 8.01, Information Technology Security

MP 8.04, Requesting Information Technology Services

MP 8.07, Security Breach of Personal Information

MP 9.03, Providing Records to the Public

MP 10.11, Communication Equipment and Service Acquisition and Use

Information Security Policy Manual

III. DEFINITIONS

A. CJI – Criminal Justice Information

B. DPPA – Driver Privacy Protection Act

C. ISA – Information Systems Administration

D. Information Technology (IT) Resources – Department computer hardware, software, services, communications, supplies, personnel, facility resources, maintenance and training.

E. PII – Personally Identifiable Information

F. Social Networking – Online community of people with a common interest who use a website or other technologies to communicate with each other and share information. Examples: Facebook, Pinterest, LinkedIn, Twitter, Instagram, etc.

G. User – Any authorized individual (including contractors and vendors) who uses Information Technology resources.

H. VPN – Virtual Private Network

IV. POLICY

The department's Information Technology (IT) resources are valuable assets and are the property of or licensed to the state. IT resources are for use by members in carrying out the department's mission. As assets, these resources must be protected and must not be used for any purpose that violates state or federal laws or rules, or for any activity which negatively effects the availability, confidentiality or integrity of these resources.

Members should have no expectation of privacy for any aspect of IT resource use. The department has the right to inspect any files created, stored, sent, received or deleted on department computers, including emails. Department email is archived and may be retrieved at any time for review.

Department smartphones and aircards are provided if a member's job duties require them and are intended to access department email and internet service for work purposes only. These devices must be used in accordance with Management Policy (MP) 8.01, Information Technology Security, MP 10.11, Communication Equipment and Services Acquisition and Use, and the Information Security Policy Manual. Use of department smartphone and aircard devices for personal reasons is strictly prohibited.

Internet access and usage is closely monitored. Members are permitted to briefly visit appropriate internet sites allowed by the department, subject to the limitations in this policy. Any personal use shall be ***brief***, ***infrequent***, and must not interfere with the member's job performance. Examples of categories of websites members may be permitted to access include:

- Google, Yahoo, etc., web search engines
- Health insurance, retirement plans, or other member benefits sites
- Wikipedia, Dictionary.com, Microsoft.com etc., informational websites
- News and weather websites

The department also reserves the right to block any inappropriate websites from user access through firewall technology. Examples of categories of websites that are deemed inappropriate include, but are not limited to, the following:

- Illegal or abused drugs
- Adult content, nudity or pornography
- Dating websites (Match.com, eHarmony)
- Gambling
- Games
- Social Networking (Facebook, LinkedIn, etc.)
- Personal Web-based Email (gmail, yahoo, hotmail, etc.)
- Any category or specific sites that host or use malware, spam, etc., or deemed unsafe by Enterprise Security Management.

Access to personal email or instant messaging on state owned devices or networks is strictly prohibitied. Supervisors are authorized to impose more restrictive guidelines in customer contact areas or for job-related reasons.

Members must be aware that all correspondence sent using the department's IT resources are considered property of the department. As such, members' correspondence may be subject to disclosure in accordance with Chapter 119, Florida Statutes, in order to comply with Florida's broad public records laws.

V. ROLES AND RESPONSIBILITIES

A. All members, contractors and vendors utilizing the department's IT resources will comply with the provisions of this policy. Failure to comply with this policy may subject members to disciplinary action.

B. Managers will ensure any vendor or contractor working in their area is aware of and complies with the provisions of this policy.

C. Each user with authorized access to IT resources will be held responsible for system security to the degree his or her job requires the use of information and associated systems.

D. All members, contractors and vendors utilizing the department's IT resources must not bypass department security measures or access IT resources for which they do not have authorization or specific consent.

E. All members, contractors and vendors utilizing the department's IT resources will comply with all department security measures established to protect confidential or sensitive information from unauthorized access or disclosure.

F. All members, contractors and vendors utilizing the department's IT resources must comply with policy as stated in MP 8.01, Information Technology Security. For a more comprehensive review of Information Technology practices and procedures, please see the Information Security Policy Manual.

G. Each member is required to annually complete and pass an online training module and acknowledge their understanding and acceptance of the responsibilities defined in the Information Security Policy Manual.

VI. PROHIBITED ACTIVITIES

Prohibited activities apply to all members, vendors or contractors when utilizing department IT resources. Prohibited activities include, but are not limited to, the following:

A. Any purpose which violates state or federal laws, rules or policies;

B. Illegal activity or any activity harmful to department computer systems, network, hardware or software;

C. Creating, receiving, accessing, downloading, installing, distributing or sending through email or the internet any of the items listed below:

1. Material containing comments, jokes, insults or negative statements about gender, race, ethnic background, national origin, religion, age or disability;
2. Material containing pornography, nudity or sexual references either implied or explicit;
3. Material containing harassing, threatening, hostile, abusive or intimidating statements;

4. Material or language containing profanity or cursing or that is vulgar, offensive or obscene (such as references to bodily functions) or otherwise inappropriate;
5. Solicitation of funds for political, religious or other personal causes. Use of email is permitted for department sponsored fundraisers;
6. Non-work related material containing graphics, pictures, sound or other media, since these items can negatively impact department computer systems by taking up storage space needed for work;
7. Chain emails asking the recipient to forward the email to others, often with the intent to receive a certain benefit (such as good luck, religious or spiritual blessings or money) and, in some cases, state that failing to send the email will break the chain and cause some negative action;
8. Software not approved or licensed by the department;
9. Instant messaging not approved or authorized by the department. ISA will maintain a list of approved Instant Messaging clients and that may be used for business purposes only. Example: Skype for Business;
10. Peer-to-peer file sharing. Example: BitTorrent;
11. Non-work related electronic discussion groups such as news groups, chat rooms or message boards;
12. Subscriptions to non-work related publications, newsletters or email alerts for personal purposes;
13. Non-work related sites discussing such topics as gambling, illegal drugs, illegal drug paraphernalia or violence;
14. Unauthorized use or viewing of copyrighted material;
15. Games, movies and music stored for personal use;
16. Screensavers, themes or wallpaper not included in the workstation operating system;
17. Access to social networking sites for non-work related activities. Examples: Facebook, Twitter, Instagram;
18. Access to streaming audio/video sites for non-work related activities. Examples: YouTube or Vimeo;
19. Access to file sharing sites or online storage sites that have not been implicitly approved for departmental use. Use of such sites to store data, including PII, CJI or DPPA data is strictly prohibited.

D. Personal gain, self-employment or secondary employment activities;

E. Using workstations, laptop computers or mobile devices to view inappropriate materials;

F. Using personal laptops or mobile devices to view inappropriate materials on state-owned or leased property;

G. Using any personal email account to conduct state business;

H. Configuring your department email account to automatically forward email to a personal, non-department or external address other than an official Tax Collector Office account;

I. Accessing, emailing, sharing, copying or distributing information from any department information systems for personal use, including but not limited to:

- Driver And Vehicle Information Database (DAVID)
- Florida Driver License Information System (FDLIS)
- Florida Real-time Vehicle Information System (FRVIS)

J. Physical or logical connection of any personal device or equipment (including vendors and contractors) to the department's computers or network, including the wireless network. Examples: personal computers, laptops, tablets, smartphones, routers or similar devices of a personal nature;

NOTE: Exceptions may be approved for remote access through the department's virtual private network (VPN) service following the procedure outlined in the Information Security Policy Manual.

K. Physical or logical connection of any personal digital storage device to a department computer, laptop or tablet. Examples: personal flash or thumb drives, hard drives, CD/DVD's or similar digital storage devices;

L. Using IT resources for remote desktop protocols (RDP) or services such as LogMeIn, RealVNC, or GoToMyPC, to connect to a personal home network or other non-business related system or network;

M. Sharing unique user credentials (UserID and passwords) with another member. User credentials are to only be used by the member to which they are assigned; and

N. Using the guest wireless service.

VII. PROCEDURES

A. Procedures for Receipt of Inappropriate Email

1. Members who receive an inappropriate email must immediately report it to their supervisor noting the date, time, sender and subject of the email. Do not forward the email to anyone unless instructed to do so by an ISA member.

2. Members should delete (do not reply to) inappropriate emails. If the member knows the sender, they should advise the sender that they

cannot receive such emails and request that their name be removed from the sender's distribution list.

3. If members suspect any emails are spam, they should be forwarded to *reportspam@flhsmv.gov* for analysis.

B. Procedures for Reporting Violations

1. Members who has reason to believe a user is in violation of this policy should immediately report the matter to their supervisor and the Bureau of Personnel Services' Office of Employee Relations at 850-617-3202 for guidance on handling the situation.

2. Supervisors are expected to advise their chain of command when they become aware of violations and contact the Bureau of Personnel Services' Office of Employee Relations at 850-617-3202 for guidance on handling the situation.

3. Bureau of Personnel Services will coordinate the review of system logs or reports with the Information Security Manager as deemed necessary.

4. Violation of this policy may result in disciplinary action up to and including dismissal.

C. Additional Procedures

For a more comprehensive review of Information Technology practices and procedures, please see the Information Security Policy Manual available on SafetyNet. Users will be required to complete annual online training to acknowledge that they understand and will abide by the department's information security policies. Notices will be sent to all members via department email at the time the online training is available.

D. Public Records Exemption

All content within the Information Security Policy Manual is confidential and exempt from public access or disclosure as specified in Section 281.301, Florida Statutes. Members or users who violate this requirement are subject to disciplinary action, up to and including termination.