| SUBJECT<br>SECURITY BREACH OF PERSONAL INFORMATION | POLICY NUMBER<br>8.07 | FLHSMV<br>FLORIDA HIGHWAY SAFETY AND MOTOR VEHICLES |
|---|---|---|
| **POLICY MAINTENANCE ADMINISTRATOR**: Information Security Manager | | |
| **PURPOSE/SCOPE:** To establish reporting procedures for the security breach of personal information. | | |

## 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 282.0041, Florida Statutes, Definitions.

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

Section 501.171, Florida Statutes, Security of confidential personal information.

Chapter 815, Florida Statutes, Computer-Related Crimes.

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

Chapter 60GG-2, Florida Administrative Code, Information Technology Security Standards.

Governor's Executive Order 19-11 on Ethics, Open Government and Preventing Sexual Harassment, effective January 8, 2019

## 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 8.03, Acceptable Use of Information Technology Resources

MP 9.03, Providing Records to the Public

MP 10.11, Communication Equipment and Service Acquisition and Use

MP 13.01, NTIS Limited Access Death Master File Compliance

Information Security Policy Manual

## III. DEFINITIONS

Breach – Unauthorized access of data in electronic form containing personal information.

Covered Entity – Governmental entity, sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information.

Customer Records – Any material, regardless of the physical form, on which personal information is recorded or preserved by any means, including, but not limited to, written or spoken words, graphically depicted, printed, or electromagnetically transmitted, that are provided by an individual in the state to a covered entity for the purpose of purchasing or leasing a product or obtaining a service.

Data in Electronic Form – Any data stored electronically or digitally on any computer system or other database and includes recordable tapes and other mass storage devices.

Governmental Entity – Any department, division, bureau, commission, regional planning agency, board, district, authority, agency or other instrumentality of the state that acquires, maintains, stores, or uses data in electronic form containing personal information.

Incident – Violation or imminent threat of violation of information technology security policies, acceptable use policies or standard security practices. Also, events that result in loss, unauthorized disclosure, unauthorized acquisition, unauthorized use, unauthorized modification, or unauthorized destruction of information resources, whether accidental or deliberate. Security incidents may include, but are not limited to, viruses, worms and Trojan horse detections, unauthorized use of computer accounts and systems, as well as complaints of improper use of information technology resources as defined in Management Policy 8.03, Acceptable Use of Information Technology Resources.

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

Personal Information –

A. An individual’s first name or first initial and last name in combination with any one or more of the following data elements for that individual:
   1. Social security number;

2. Driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;
3. Financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;
4. Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
5. An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

B. User name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

C. The term "personal information" does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

<u>Third-party agent</u> – Entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity or governmental entity.

<u>Threat</u> – Any circumstance or event that has the potential to adversely impact the department's operations or assets through an information system via unauthorized access, destruction, disclosure, or modification of information or denial of service.

## IV. POLICY

The personal information contained in the department's information systems, which includes, but is not limited to, the personal information contained in the motor vehicle and licensing records, will be protected. Each covered entity, governmental entity or third-party agent must take reasonable measures to protect and secure data in electronic form containing personal information.

## V. ROLES AND RESPONSIBILITIES

A. The Technical Assistance Center (TAC) serves as the department's single point of contact for data breaches.

B. The Information Security Manager (ISM) serves as the liaison between the Executive Leadership Team (ELT) and the Incident Response Team (IRT).
C. The ELT represents the leaders of the department as defined in the Enterprise Security Computer Security Incident Response Manual (confidential for use by ELT and IRT only).

D. The IRT is comprised of key department personnel as defined in the Enterprise Security Computer Security Incident Response Manual.

E. The ELT and IRT will convene as needed to address security breaches and associated issues.

## VI. PROCEDURES

For additional procedures regarding information technology and security, please see Procedures for Security Breach of Personal Information and the Information Security Policy Manual.