Ohio Department of Public Safety
Division: DPS
Policy: DPS-200.05 PROTECTING SENSITIVE INFORMATION
Revision #: 6 **Approved Date:** 6/15/2022
Security: No Restrictions-Available for Public Release
Distribution:

Summary of Revisions

Changed name from *Operational Security (OPSEC)* to *Protecting Sensitive information*.

Complete rewrite, combined with DPS-200.06 *Collection and Destruction of Documents and Other Media Containing Sensitive Information (OPSEC)* and DPS-801.02 *Accessing Confidential Personal Information (CPI)*

Purpose

To establish guidelines to ensure that any item generated or received by DPS (including but not limited to paper documents and non-paper media) that contains sensitive information, is collected, processed, maintained, and securely destroyed to safeguard against loss, unauthorized access, use, or disclosure.

To establish guidelines to ensure operational security of sensitive information.

Policy

I. STATEMENT OF POLICY

A. This policy applies to all DPS Divisions, including all DPS field offices and Highway Patrol posts.

B. The security of sensitive information is the responsibility of each DPS employee and anyone who has been given access to sensitive information.

C. Sensitive information shall be suitably protected from unapproved disclosure to other employees and the public.

D. Records and correspondence shall be retained and disposed of in accordance with Ohio Revised Code (R.C.) Chapter 149, approved record retention schedules filed with the Department of Administrative Services, DPS directives, and other applicable state and federal statutes, regulations, and directives.

E. This policy is not intended to interfere with the administration of requests for public records in accordance with R.C. 149.43. Questions regarding whether a request is a public records request, a request for non-public records, or a request for confidential personal information should be directed to Legal Services.

II. CONTACTS

Facility Services

- Shipley - (614) 644-1256
- Alum Creek (ACF) – (614) 752-7293
- Emergency Management Agency (EMA) – (614) 889-7166

Distribution and Inventory Services (DIS) - (614) 752-7908

DPS Service Desk – (614) 752-6487

Post 98 - (614) 752-6007

Security Operations Group – (614) 752-7686

Legal Services – (614) 466-7014

III. DEFINITIONS

A. Access - An opportunity to copy, view, or otherwise perceive whereas "access" as a verb means to copy, view, or otherwise perceive.

B. Adversary - Anyone who may be collecting information about the Department and intends to use this information to defeat operations or plan an attack. Adversaries can be organized into eight major groups:

- criminals,
- organized crime and drug trafficking,
- international terrorists,
- domestic militia,
- extremist and cults,
- foreign intelligence agencies,
- hackers and crackers, and
- disgruntled or dishonest employees.

C. Computer System - A "system," as defined by R.C. 1347.01, that stores, maintains, or retrieves personal information using electronic data processing equipment.

D. Electronic Records – R.C. 1306.01(G) a record created, generated, sent, communicated, received, or stored by electronic means. A record or contract that is secured through blockchain technology is considered to be in an electronic form and to be an electronic record.

E. Individual - Natural person or the natural person's authorized representative, legal counsel, legal custodian, or legal guardian.

F. Personal Information System - A "system" that "maintains" "personal information" as those terms are defined in R.C. 1347.01. "System" includes manual and computer systems.

G. Records – R.C. 149.011(G) "Records" includes any document, device, or item, regardless of physical form or characteristic, including an electronic record, created or received by or coming under the jurisdiction of any public office of the state or its political subdivisions, which serves to document the organization, functions, policies, decisions, procedures, operations, or other activities of the office.

H. Sensitive Information

Includes, but is not limited to:

- Confidential personal information, which is any personal information that is not a public record(*e.g.*, Social Security Number, tax identification number, or medical or disability information, and, other personal information when under the specific circumstance is not subject to disclosure as a public record, such as an individual's date of birth, driver license number, or state identification card number);
- Photograph or digital image of the Bureau of Motor Vehicles
- law enforcement and Homeland Security sensitive information;
- specific emergency operations plans which may cause a security risk(e.g., Active Aggressor plan, Threat Hazard Identification Risk Assessment, and Hazard Identification Risk Assessment);

- any information exempted from "Public Record" by R.C. 149.43;
- any information that can be used to access financial resources, such as bank account numbers, credit or debit card numbers, EFT numbers, etc.; and
- other personal information required by law to be maintained in a secure manner.

I. Threat - Any person, organization, or country that has the intent and technical capability to attack the Department by exploiting vulnerabilities.

J. Vulnerabilities - DPS employees, stakeholders, property, and sensitive information.

IV. OPERATIONAL SECURITY (OPSEC)

OPSEC is a risk management tool used to deny adversaries information concerning the Department's intentions and capabilities by identifying, controlling, and protecting indicators associated with the planning and execution of law enforcement and public safety missions. The OPSEC process consists of five parts:

- Identifying Critical Information,
- Conducting a Threat Analysis,
- Performing Vulnerability Assessments,
- Assessing Risks, and
- Applying Countermeasures.

These are not steps to be followed in a sequential, linear fashion but a fluid process that allows employees to use the system in a manner that fits the particular situation.

V. TECHNIQUES AND METHODS OF COLLECTION OF INFORMATION BY ADVERSARIES

A. Techniques - Adversaries collect intelligence by determining the, "how, who, when, what, and where" of the Department:

- HOW is DPS organized? HOW does it operate?
- WHO are the organizational leaders?
- WHEN is DPS most vulnerable?
- WHAT type of intelligence capability and secure communications does DPS have?
- WHERE is DPS located? WHERE is DPS most vulnerable?

B. Intelligence Methods - Intelligence methods used include:

- open source research;
- public domain technical reports;
- people;
- communications;
- photography;
- trash; and
- surveillance.

VI. OPERATIONAL SECURITY TECHNIQUES AND RESPONSIBILITIES

A. Open Source Information and Public Domain Reports

- All media relations shall be referred to the DPS Communications Office.
- Public records requests and public domain reports shall be thoroughly reviewed prior to release of information. Refer to DPS-400.04 Administration of Public Records Requests for more information regarding public records requests.
- Extra care should be taken to ensure sensitive information is not being released to the public if it is exempt from public record, per R.C. 149.43.

B. People

- Employees must have identification visible on their person at all times. Employees shall also be watchful of unauthorized persons entering and exiting DPS buildings and locations.
- Employees shall not share personal computer, network, database, and internet or intranet accounts and/or passwords.
- Employees will not be permitted remote-access to DPS networks unless authorized by the DPS Information Technology Security Officer.

C. Communications

- Employees shall be aware of their surroundings and exercise due caution when conveying sensitive information over public e-mail, fax, landline telephone, cellular telephone, or radio.
- Communicated sensitive information sent outside of DPS shall be encrypted, and communicated sensitive information being sent within the department should be encrypted when possible.

D. Photography

- Employees shall be cautious when taking photos in or on DPS properties.
- Employees must be cautious of others taking photos of or at DPS facilities.

E. Trash/Records Disposal

- Employees must follow all DPS records management and retention policies and procedures.
- Employees must follow all DPS policies and procedures regarding the disposal of trash and secure documents.

F. Employee Surveillance

- Employees must be aware of their surroundings and alert to the potential of surveillance (if an employee becomes aware of or suspects surveillance, it should be reported to Post 98 or the local Highway Patrol post).
- Sensitive, proprietary information should never be discussed in public areas. Conversations in elevators, restrooms, service areas, and over cellular telephones should be conducted with the thought of OPSEC in mind.
- Computer screens, sensitive paperwork, telephone screens, and other media should be protected from public view.

VII. TRAINING - ALL EMPLOYEES

A. All employees and anyone with access to DPS sensitive information are required to complete all assigned on-line OPSEC and sensitive information training.

B. Each employee is required to sign-off on any assigned policy that relates to OPSEC and sensitive information as soon as possible.

VIII. LOGGING ACCESS

R.C. 1347.15 requires DPS to include a mechanism for recording or logging specific access by its employees to confidential personal information and the legitimate reasons for DPS to store and maintain confidential personal information.

The DPS Director and each member of the Director's senior advisors who access or direct another employee to access confidential personal information from a personal information system shall manually log that access. The access of confidential personal information by all other DPS employees shall be automatically logged or recorded by the computer system.

Exemptions to Logging - The logging requirements set forth in this policy shall not apply:

A. When confidential personal information is accessed as a result of a request of the person whose information is being accessed.

- A request from an individual's authorized representative should be considered as a request from the individual. An authorized representative can be legal counsel, legal custodian, or legal guardian of the individual.
- If an individual requests that an employee take some action on the individual's behalf, and the employee needs to access the sensitive information to accomplish the actions; there is an inherent authorization by the individual to access sensitive information. An example of this is a person filling out an application or renewing a license.

B. When the DPS employee comes into incidental contact with confidential personal information and the access of the information is not specifically directed toward a specifically-named individual or a group of specifically-named individuals.

C. When access to confidential personal information occurs as a result of routine office procedures and the access is not specifically directed toward a specifically-named individual or group of specifically-named individuals.

- This exemption will apply primarily to Human Resource (HR) records on employees as long as the information would not adversely affect a person.
- This is a very narrow exception and applies to HR information about individuals internal to DPS. Medical information in support of an employee's leave request under FMLA would fall under this exclusion, but background checks on job applicants would not be excluded.

D. The DPS Information Technology Office (ITO) shall ensure that any upgrades to an existing computer system or the acquisition of any new computer system that stores, manages, or contains confidential personal information include a mechanism for recording specific access by DPS employees to sensitive information.

IX. SCOPE OF ACCESS

Valid Reasons for Accessing sensitive information (Ohio Administrative Code [OAC] 4501-55-03)

The requirements of R.C. 1347.15 (B)(2), administrative rules, and this policy contain valid reasons, directly related to the Department's exercise of its powers or duties, for which only DPS employees may access sensitive information.

A. Performing the following functions constitute valid reasons for authorized DPS employees to access sensitive information:

1. responding to a public records request;
2. responding to a request from an individual for the list of sensitive information DPS maintains on that individual;
3. administering a Constitutional provision or duty;
4. administering a statutory provision or duty;
5. administering an administrative rule provision or duty;
6. complying with any state or federal program requirements;
7. processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;
8. auditing purposes;
9. licensure [or permit eligibility, filing, etc.] processes;
10. investigation or law enforcement purposes;
11. administrative hearings;
12. litigation, complying with an order of the court, or subpoena;
13. human resource matters (e.g., hiring, promotion, demotion, discharge, salary/compensation issues, leave requests/issues, time card approvals/issues);
14. complying with an executive order or policy;
15. complying with Department policy or a state administrative policy issued by the Department of Administrative Services, the Office of Budget and Management, or other similar state agency;
16. complying with a collective bargaining agreement provision; or
17. in order to carry out specific duties of DPS.

Questions regarding whether access for a specific purpose falls within the Department's powers, duties, and responsibilities should be directed to DPS Legal Services.

B. CAUTION: Accessing sensitive information for any purpose other than as delineated in this policy is strictly prohibited. This includes, but is not limited to, accessing sensitive information for "curiosity purposes" in regards to persons or groups of persons that an employee may personally know, or knows of due to the person or groups of persons being in the media, holding elected or appointed positions, or having achieved a certain amount of fame or notoriety.

X. REQUESTS FOR SENSITIVE INFORMATION

A. Written Requests for Confidential Personal Information - R.C. 1347.15 requires DPS to respond to a written request from an individual for a list of confidential personal information maintained by DPS about the individual. An individual may make a written request for a list of the confidential personal information kept by DPS about the individual by completing and submitting a notarized *Request for Confidential Personal Information Affidavit* (DPS 0023). If the individual is a legal guardian, the individual must also present a certified copy of the court entry appointing him or her legal guardian. If the individual is an authorized representative, the individual must also present a notarized power of attorney form. Forms may be delivered in person to the DPS public entrance police officer desk located at 1970 West Broad Street, Columbus, OH 43223. Forms may also be mailed to: Ohio Department of

Public Safety Legal Services Office, PO Box 182081, Columbus, OH 43218- 2081.

If the form is delivered in person, the police officer who receives the document will forward the document to Legal Services for processing.

1. Response - Upon receipt of the completed *Request for Confidential Personal Information Affidavit* (DPS 0023) Legal Services shall record the request and review to ensure that it is notarized and the information required has been provided. If not notarized or if the information is incomplete, the *Request for Confidential Personal Information Affidavit* (DPS 0023), along with a statement that the request was improperly submitted, shall be sent to the requestor. If the form is notarized and properly completed, Legal Services shall send an acknowledgement letter to the requestor stating that their request has been received and is in the process of being filled. DPS Legal Services shall send the request to the appropriate Public Records Administrator (PRA) for processing by each DPS Division/Office. Although such requests are not considered public records requests, the PRAs are responsible for processing them. The PRA will, within a reasonable time period, coordinate the search and retrieval of the confidential personal information that is on file within their Division/Office and return the results to Legal Services. All results should be forwarded to Legal Services for review regardless of whether such results fall into one of the exceptions listed below.

   Once all applicable Divisions have responded to the request, Legal Services shall review the information and determine what information will be released in compliance with R.C. 1347.15. They will then send a response letter containing the information available for release to the requestor. Confidential personal information shall not be released when:

   - It relates to an investigation about the individual.
   - It is part of a confidential law enforcement record, investigatory record, or trial preparation record.
   - It is maintained in a database owned by a Division that is exempted from R.C. Chapter 1347, as indicated in 1347.04 (A)(1)(a) through (e).

   If all information relates to an investigation about the person or any of the other exemptions listed above, Legal Services shall inform the requestor that DPS has no confidential personal information that is subject to disclosure. In all other cases, the response letter from Legal Services will:

   - Outline the exact confidential personal information on file,
   - Notify the requestor that the requestor has the right to dispute information under R.C. 1347.09,
   - Refer the requestor of the requestor's rights under R.C. 1347.08, and
   - Advise the requestor to refer any questions to Legal Services, who shall provide a contact number and e-mail address in its response.

2. Costs - DPS intends to charge all requesters the appropriate costs allowed by law for providing a list of confidential personal information. Such costs do not include the cost of labor involved in preparing the list. Prior to releasing responsive records, Legal Services shall determine whether to require pre-payment.

3. Improper Requests - Any employee may make a confidential inquiry to Legal Services regarding the appropriateness of direction from a senior official to access confidential personal information about a specific individual or group of specifically named individuals. Any employee who becomes aware of an inappropriate access or direction to

access confidential personal information shall notify the Security Operations Group immediately.

XI. PASSWORDS

Each employee authorized to access sensitive information shall have a unique user ID and password, and each employee shall be responsible for transactions conducted using that user ID and password. All passwords shall conform to existing federal and state laws, regulations, and DPS-800.01 *IT User Guidelines*.

XII. PAPER DOCUMENTS CONTAINING SENSITIVE INFORMATION

DPS keeps many paper documents that contain sensitive information. To control access to these documents, the following protective actions are required:

A. All documents containing sensitive information shall be stored in locked file cabinets, locked desk drawers, or other secure storage when not in use. These documents shall not be left on work surfaces, desktops, or unsecured in cubicles when the employee is not in the work area.

B. Record retention boxes orders generated by the Record Center will be delivered and picked-up by the DIS Transport/Salvage Unit, and must be properly verified and secured by the DIS Shipley Receiving and DIS EMA Receiving staff prior to delivery to and from the requesting business unit manager.

C. Business unit managers shall issue keys for the cabinets to only those employees having a need to access these documents.

D. Treat mass storage devices such as CDs, DVDs, and thumb drives containing sensitive information the same way by placing them in secure storage.

XIII. DISPOSAL OF SENSITIVE INFORMATION

A. Locked Containers - Secure containers are provided for depositing sensitive documents that must be shredded before recycling.

B. Container Markings and Location - Collection containers for sensitive documents shall be clearly identified and located as jointly determined by Facility Services and office components based on their volume.

C. Container Pick-up - Containers shall be picked up from designated collection points throughout the facilities when full. To arrange for a special pick up or to increase the frequency of pick-ups, contact the appropriate building Facility Services.

D. Disposal and Documentation - All documents deposited in the secure shredding containers will be transported to the ACF by DIS and securely stored until picked up by the document destruction contractor. The contractor shall be certified by the National Association for Information Destruction (NAID) and shall handle and destroy documents in accordance with national standards set by NAID. The contractor shall provide a Certificate of Destruction for all materials picked up and destroyed to DPS.

E. Destruction of Other Media - Contact the Record Center to arrange the destruction of microfilm, data tapes, audio tapes, video tapes, and other non-paper sensitive items.

F. Recyclables - Recyclable paper products that do not require shredding shall be placed in the blue "Recycle Ohio!" recycling containers provided by Facility Services upon request. Examples of paper that does not require shredding include obsolete forms, envelopes, publications, scrap paper, etc. All paper placed in the recycling containers shall not contain sensitive information.

- The EOC uses a private contractor for paper recyclables.

G. Shredding Large Volumes of Sensitive Materials - Contact DIS to make arrangements for shredding of large volumes of paper containing sensitive information.

H. Requesting Unlocking of Container - Contact the appropriate building Facility Services to request a collection container be unlocked to retrieve any documents once they are deposited in the collection containers.

XIV. DPS FIELD OFFICE/PATROL POST PROCEDURES

A. Each DPS Field Office/Patrol Post shall handle documents containing sensitive information in one of two ways:

- give extra, unneeded copies of documents containing sensitive information directly to the customer; or
- shred, or otherwise destroy, all unneeded copies of documents containing sensitive information, including extra copies of, and carbon paper from, any documents that contain sensitive information. Each DPS Field Office/Patrol Post is responsible for ensuring these documents are destroyed in a manner which will render the sensitive information unusable.

B. Each DPS Field Office/Patrol Post shall ensure that non-paper items such as facsimile machine or printer imaging cartridges that contain images of sensitive information (e.g., driver license images) are properly destroyed.

XV. RESPONSIBILITIES

A. Supervisors

- Monitor office component and employee compliance with the provisions of this policy and ensuring that all documents containing sensitive information are deposited in designated collection containers or shredded before being deposited into a recycling bin.
- Ensure that records are not deposited into designated collection containers before their retention period expires.
- Submit a *Certificate of Records Disposal* (DPS 0131) through their Division's Records Management Coordinator (RMC). Certificates of Records Disposal shall be completed as records are destroyed and the certificates shall be immediately submitted to the designated Division/Section RMC. RMC's will forward collected certificates to the DPS Record Center on the last business day of every month.

B. Record Center

- Retain *Certificates of Records Disposal* (DPS 0131) in accordance with the form's records retention schedule (SAN 760-1088).
- Ensure all records that are stored in the Record Center are destroyed when the retention period expires and the record owner approves removal and subsequent destruction. Record owners shall return all obsolete records requested from Record Center storage back to the Record Center for destruction so the "on loan" status can be updated and destruction documented.

XVI. CONFIDENTIALITY STATUTES, RULES, AND REGULATIONS

Employees should review O.A.C. Rule 4501-55-05 to reference a list of federal and state statutes, regulations, and administrative rules that make personal information maintained or used by the Department confidential.

XVII. PENALTIES FOR UNAUTHORIZED ACCESS AND/OR MISUSE OF SENSITIVE INFORMATION

A. R.C. 1347.15 stipulates:

- No person shall knowingly access sensitive information in violation of a rule of a state agency.
- No person shall knowingly use or disclose sensitive information in a manner prohibited by law.
- No state agency shall employ a person who has been convicted of or pleaded guilty to a violation of the above-listed offenses.

B. Violations of the R.C. and this policy may result in:

- criminal prosecution,
- civil liability for the employee,
- termination,
- prohibition of employment with the State of Ohio for the employee's lifetime.

XVIII. SUBJECT MATTER EXPERTS

Questions related to this policy should be directed to the following:

Office	Name	Phone	Email
Legal Services	Anne Vitale	(614) 387-0414	apvitale@dps.ohio.gov

Form and Supplemental References:

Request for Confidential Personal Information Affidavit (DPS 0023) - http://jp-intweb.ps.dps.state.oh.us/crs/

Standard References:

Related Policies:

DPS-400.04 ADMINISTRATION OF PUBLIC RECORDS REQUESTS
DPS-800.01 IT USER GUIDELINES

Attachment(s):