DFS INFORMATION SECURITY POLICY

DFS is entrusted with confidential, sensitive, and personal information not for the public domain, whose unauthorized disclosure could be prejudicial to DFS personnel, the District of Columbia and its citizens. In the interest of maintaining the highest level of information security, this policy clarifies what constitutes "confidential, sensitive and personal information," how such information must be managed, and the consequences of breaching this policy.

1. **Persons Affected:**
   This policy applies to ALL DFS personnel, including employees, contractors, detailees, interns, researchers and consultants that have, or may acquire, access to DFS's information resources and those with responsibility for maintaining DFS information. ALL personnel must sign an INFORMATION SECURITY AGREEMENT.

2. **Definitions of Confidential, Sensitive, and Personal Information**
   DFS acquires and maintains confidential, sensitive and personal information that is accessed on paper and in electronic or computer-based files, software, accounts and documents, as well as through face-to-face discussions. This includes information developed by personnel, alone or with others, or entrusted others.
   - **Confidential Information** is information that is exempt from public disclosure under the provisions of section 2-534 of the District of Columbia's Annotated Code or other applicable State or federal laws. This may include information regarding investigations, Public Health, Forensic Science, Crime Scene Investigation, Death Investigation, etc. Furthermore, confidential information may include, without limitation, information relating to the finances, personnel records, business and strategic plans of DFS.
   - **Sensitive Information** is information that requires special precautions to protect it from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive information may be either public or confidential, and normally requires a higher assurance of accuracy and completeness, including:
     - Copyrighted, trademarked or patented materials, images and information;
     - Contractual documents such as subcontractor/contractor agreements, request for proposals, grant contracts, memoranda of understanding/agreement; and
     - Human resources and accounting documents such as financial records, income tax returns, wage and tax statements, bank statements, organizational budgets, payroll statements, and credit card statements.
   - **Personal Information** is personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. This information must be protected from inappropriate access, use or disclosure. Personal information is further defined as:
     - **Notice-Triggering Personal Information** – specific items or personal information (employee name plus social security number, taxpayer ID number, date of birth, financial account information, forensic DNA profile, baseline blood samples, vaccination records, or employee badge) that may

trigger a requirement to notify individuals in the event of unauthorized disclosure; and

- **Protected Health Information** – individually identifiable information created, received or maintained by such organizations as health care payers, health care providers, health plans and contractors to these entities, in electronic or physical form.

3. Guidelines for Information Regarding Investigations

Any information regarding investigations is not to be discussed outside the respective department(s), except as authorized by law.

- Personnel may discuss information regarding investigations with law enforcement officers assigned to the case, as appropriate.
- Personnel may discuss information regarding investigations with prosecutors and defense attorneys assigned to the case.
- Personnel may discuss information regarding investigations with the Center for Disease Control as mandated by law.
- Personnel may discus autopsy findings with those authorized by law.
- Personnel may discuss finances, business and strategic plans with other agencies provided discussions are consistent with the normal course of business.
- Personnel may not discuss any of the above information with persons not associated with the case.
- Personnel are specifically cautioned about social media. Personnel may not post photos; information regarding investigations, whether true or not; commentary on how a case is being investigated; test results; or any other commentary about cases; etc; on any social media sites, including but not limited to Instagram, Vine, Keek, Tumblr, Pintrest, Facebook, Twitter, personal blogs, instant message of any kind; message boards; email groups; Yahoo groups.

4. Guidelines for Managing, Sharing, Securing and Destroying Information

The DFS Director has tasked the Human Resources Division with reviewing information security procedures with new employees and contractors. The use of data from the Department of Forensic Sciences and/or the Office of the Chief Medical Examiner and/or Public Health is limited exclusively to those purposes authorized by DFS and/or OCME and/or PHL; D.C. Code Title 5, Chapter 15; Title 5, Chapter 14; and Title 7 Chapter 2A; as well as other applicable Federal and District Laws. DFS personnel must routinely implement the following safeguards to prevent unauthorized use or disclosure of information:

- Secure printed information in locked rooms or cabinets;
- Do not leave information in places, such as unsecured desks or conference rooms, where unauthorized persons could access it;
- Lock computer screens and other technology devices when leaving office or desk space. This includes laptop computers, personal mobile devices, and cellular phones;
- Do not share electronic usernames or passwords. Guests requiring computer access should speak to IT support to obtain credentials;
- Do not leave laptops, mobile media devices, cell phones or paper documents in automobiles;
- Shred documents with sensitive information instead of throwing them in the garbage;

- Double-check fax numbers and email addresses; coordinate a system to confirm receipt by the recipient;
- Avoid communicating sensitive information (*e.g.*, social security numbers) via formats that leave a trail; make a telephone call instead.
- When possible, use registered mail to send information to confirm it wasn't intercepted or delivered to the wrong party;
- Do not store confidential, sensitive, or personal information on non-encrypted laptops or mobile devices;
- Do not backup data to non-encrypted media such as diskettes, memory sticks, or CDs; contact IT support for access to group drives remotely;
- Ensure that agreements with vendors or other sub-contractors include assurances to appropriately prevent information security breaches; and
- Under no circumstances can investigative or case sensitive information be displayed on any social media site. Personnel are specifically cautioned about social media. Personnel may not post photos; information regarding investigations, whether true or not; commentary on how a case is being investigated; test results; *or any other commentary about pending cases* etc; on any social media sites, including but not limited to Instagram, Vine, Keek, Tumblr, Pintrest, Facebook, Twitter, personal blogs, instant message of any kind; message boards; email groups; Yahoo groups.

5. Notification and Enforcement

DFS recognizes that information may unintentionally be disclosed without authorization. In these circumstances, prompt notification of the disclosure is essential.

- **Notification Requirements**
  Unintentional disclosure of information in any format must be reported immediately. Notify your direct supervisor or human resources personnel of any loss or theft of confidential, sensitive, or personal information in any format.
- **Consequences of Purposeful Disclosure of Information**
  Any DFS personnel who engage in the unauthorized use, misuse or disclosure of DFS's confidential, sensitive or personal information will be subject to administrative sanctions up to and including immediate termination of employment, and may be subject to civil or criminal prosecution. Administrative sanctions will be imposed in accordance with the Table of Appropriate Penalties provided in Chapter 16 of the District Personnel Manual.

If you have any questions about DFS's information security policy, consult your direct supervisor or the Human Resources Division.

GOVERNMENT OF THE DISTRICT OF COLUMBIA
VINCENT C. GRAY, MAYOR

DEPARTMENT OF FORENSIC SCIENCES
CONSOLIDATED FORENSIC LABORATORY
401 E STREET SW WASHINGTON, DC 20024

DFS INFORMATION SECURITY AGREEMENT

I have read the DFS Information Security Policy. I understand what constitutes "confidential, sensitive and personal information," how such information must be managed, and the consequences of breaching this policy.

By my signature below, I agree to abide by the guidelines for managing, sharing, securing and destroying DFS information to prevent the unauthorized use, misuse or disclosure of information. Further, I understand the notification requirements in the event of unintended information disclosure, as well as the potential administrative, civil and/or criminal consequences of purposeful disclosure of confidential, sensitive and personal information.

_____ _____

Employee Signature Date

_____

Employee Name, Printed