U.S. Virgin Islands Division of Personnel

EFFECTIVE SEPTEMBER 9, 2024:

EMPLOYEE CONFIDENTIALITY POLICY

Purpose

All Division of Personnel (DOP) employees perform services for DOP that may require DOP to grant access to and/or disclose confidential/proprietary information ("Confidential Information") to employee. As such, the purpose of this Notice is to ensure that all DOP employees understand their obligation to protect the confidential information encountered during their employment at DOP.

Definition

For the purposes of this policy, "Confidential Information" includes but is not limited to:

- Personal information, including social security numbers, home addresses, phone numbers, and personal email addresses;
- Employment records, including applications, resumes, performance reviews, disciplinary records, and compensation details;
- Medical and health information;
- Legal documents and correspondence;
- Financial Data;
- Proprietary and business information that is not publicly available;
- Information of any kind concerning any matters affecting or relating to, the business or operations of DOP, and/or the processes, or data of which DOP has a direct interest and not known or available outside of DOP and/or the Government of the Virgin Islands (GVI);
- Any other information designated as confidential by DOP; and
- DOP shall have the sole right to determine the treatment of all writings, ideas and discoveries received from employees during employment with DOP.

Obligations

To protect the Confidential Information that will/may be disclosed during employment, employees shall:

A. Hold the Confidential Information received from DOP in strict confidence and will exercise a reasonable degree of care to prevent unauthorized disclosure to others. (i.e. securely storing/safeguarding confidential information, etc.);

B. Use confidential information only in an official capacity and to further legitimate government interests.

C. Not disclose or divulge either directly or indirectly GVI Confidential Information to others unless first authorized to do so in writing by authorized personnel within DOP;

D. Not reproduce Confidential Information nor use this information commercially or for any purpose other than the performance of duties for DOP;

E. Upon request or upon termination of relationship with DOP, deliver to DOP any notes, documents, equipment, and materials containing Confidential Information received from DOP or originating from employment with DOP and shall not retain any copies, or other reproductions, in whole or in part.

F. Be strictly prohibited from using unauthorized channels (i.e. personal email accounts and messaging apps) to disseminate, discuss, or transmit official DOP communications. Authorized channels are those approved and provided by DOP, (i.e. official email accounts, secure messaging systems, and designated collaboration platforms).

Permitted Disclosures

Employees may disclose Confidential Information as follows:

- To other employees or agents of DOP who have a legitimate need to know while performing job duties.
- When required by law or in response to a valid court order or subpoena, provided that employee promptly notifies DOP of such requirement and cooperates with any efforts to limit the disclosure.
- When doing so (i) in confidence to a federal, state or local government official, either directly or indirectly, or to an attorney and (ii) solely for the purpose of reporting or investigating a suspected violation of law.
- When in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made (i) under seal and (ii) does not disclose the confidential information.

Domain Access Conditions/Acceptable Use

To protect the DOP Domain and Information Technology that will/may be used/accessed during employment the following rules apply:

- Credentialed access to DOP domain connected devices shall not be revealed or shared to anyone in or outside the agency. Employee is responsible for ensuring that these credentials remain private. Credentials should be changed at 75-day intervals with a unique seven characters or greater password.
- Network access will be solely for use in conducting DOP business.
- Software programs not belonging to or authorized by DOP, shall not be installed on any DOP computers or mobile devices without the express consent of authorized HRIT (Human Resources Information Technology) manager.
- No software program owned by DOP or that DOP is authorized to use will be removed or transferred without the express consent of authorized HRIT manager.
- Device configuration, including installed software/drivers, should not be modified without the express consent of authorized HRIT management.
- Employee understands that DOP reserves the right to monitor or access any DOP property, including electronic or telephonic and these systems may be monitored when there is a legitimate business purpose. Employee should have no expectation of privacy in using GVI equipment.
- Revocation of DOP Domain access is at authorized management's discretion.

Reporting Violations

Any suspected or actual violations of this policy must be reported immediately through our Ethical Reporting Form. The DOP Ethical Reporting Form can be accessed by visiting the Division of Personnel website at dop.usvi.org, select Employees, select Documents and Forms, and then select Ethical Reporting.

Duration of Obligations

Employee's obligations under this policy shall continue:

- For as long as employee is employed by DOP.
- After the termination of employee's employment with DOP, regardless of the reason for termination, for a period of two years thereafter.

Consequences of Violations

DOP reserves the right to take disciplinary action, up to and including termination, for any violation of this agreement.

Approved by:

Cindy L. Richardson

Director
Division of Personnel

_8/5/2024_

Date