VI Department of Finance

Management Information System (MIS) Division

Policies and Procedures

SOPP 420 – Information Technology Resource Regulation and Acceptable Use Policy

SOPP SECTION ORDER

SOPP NO. / Title:
SOPP 420 – Information Technology Resource Regulation and Acceptable Use Policy
Effective Date:
Effective 10/1/2025
Approved Date:
Approved 10/23/2025
Approved By:
Commissioner of Finance

Section 1. PURPOSE:

To present a clear understanding of the responsibilities of the end user and the establishment of acceptable behavior regarding use of the Department of Finance's (DOF) information technology resources. This SOPP shall be reviewed and revised, if necessary, at a minimum of every two years from its effective date to ensure its continued relevance and accuracy.

Section 2. SCOPE:

This policy applies to all users of the electronic network and systems provided by Virgin Islands' DOF.

Section 3. ROLES AND RESPONSIBILITIES:

Department / Position	Role
Department of Finance (DOF) – Management Information Systems (MIS) Division	Administer and oversee all of the Department's IT systems.
IT Resource Users	Comply with MIS policies

Section 4. DEFINITIONS / ABBREVIATIONS:

SOPP Acronyms	
D&A – Department and Agency	DOF – Department of Finance
FTP – File Transfer Protocol	FMS – Financial Management System
PO – Purchase Order	T&A – Time & Attendance
IT – Information Technology	ERP – Enterprise Resource Planning System

Section 5. REGULATIONS / REFERENCES:

None.

Section 6. POLICY:

6.1 ACCEPTABLE USE

By participating in the use of the electronic network and systems provided by Virgin Islands Department of Finance (DOF), users agree to comply with policies governing their usage. These resources include the Enterprise Resource Planning (ERP) System, TimeForce and

Time & Attendance (T&A) – the Standard Automated Time and Attendance System (STATS), the (legacy) Financial Management System (FMS) and internet services. The following comprises the *Acceptable Use Policy* requirements to be observed while utilizing DOF's information technology (IT) resources:

1. Users shall use the Department's IT resources for intended purposes only;
2. Acceptable use must be legal, ethical, reflect honesty, and show restraint in the consumption of shared resource;
3. When logged into any of the DOF IT resources, users shall conduct themselves in a manner that is appropriate and proper as representatives/employees of the Government of the United States Virgin Islands;
4. Users shall not use any DOF system to send, receive, view or download any illegal materials or engage in any other illicit act;
5. Users shall not download or transmit files larger than 500MB unless absolutely necessary for financial administration and/or enforcement purposes; if necessary, users shall download the file at a time when the system usage is low, i.e., generally after standard business hours (weekends, or after 5:00pm weekdays);
6. No user has unlimited use of the network infrastructure. Bandwidth is compromised when users frequently traverse (surf) the internet, downloading excessively large files, music, video clips, or audio and video streaming. Thus, excessive use thereof is prohibited. Live audio or video streaming during peak productivity hours is prohibited, unless it is immediately required, for work-related training, or financial processing administration;
7. Any usage of IT resource in which acceptable use is questionable should be avoided. When in doubt, seek policy clarification prior to pursuing the activity; and
8. DOF reserves the right to revise the *Acceptable Use Policy* to keep pace with changing and evolving information technology.

a. System / Information Integrity

9. Users should not sabotage the ERP, STATS, FMS or any other IT resources of the Department of Finance;
10. Users shall not deliberately attempt to disrupt DOF systems performances or destroy data by any malicious means, including unnecessary interference with equipment, cabling, or files, or by spreading computer viruses, spyware, malware or other software intended to disrupt proper functioning of equipment and peripherals, and IT services;
11. No user, under any circumstances should alter, attempt to alter or install any software code, (programs, compiled or un-compiled objects) or reverse engineer any software on any of DOF systems, unless DOF Management Information Systems (MIS) division authorization has been granted;
12. Use of network utilities for the purpose of gaining network sensitive information from (probing or scanning, phishing, spoofing) DOF IT systems or network is prohibited;
13. Users shall not maliciously populate the ERP, STATS or FMS with any inaccurate and/or frivolous data whatsoever. Data entry should be accurate, and reflect proper transaction processing guidelines and SOPPs;

14. Users shall not intentionally disseminate inaccurate financial information to any individual or entity, nor shall users be at liberty to disseminate financial information to any individual or entity, unless appropriate authorization is granted. All requests for financial information to be derived from the ERP, STATS or FMS must adhere to this *Information Technology Resource Regulation* – 'Services' section. Any attempt to fraudulently extract and disseminate financial information is strictly prohibited;
15. Users are strictly prohibited from global inquiries on the ERP, STATS, or FMS, which may generate information that is not relevant to his/her functional duties. Such information is relevant only to selective others on an as needed basis;
16. Apart from the user's own employee records, no attempts shall be made to extract any personnel, vendor or other financial records for personal or private use without direct and appropriate authorization;
17. Special access has been (or will be) granted to selective staff in your department to generate reports for retroactive payrolls in order to enable proper reporting, particularly, given conditions of employee separation (through retirement, transfers or resignation/ termination) from your department/agency. Departments and agencies staff with privileged access are prohibited from conducting global queries or applying location codes outside of the respective department/agency. Therefore, the use of queries is limited to the payroll locations codes or G/L equivalent codes when performing reconciliations for your department or agency.

b. Security

18. Users must immediately change all temporary passwords provided by MIS; users must change their password when the system requests it, or at any time the user deems necessary to ensure system security;
19. Users are responsible for the use of their individual account and should take all precautions to safeguard their login information from others;
20. Users shall provide their passwords to no one, under any circumstance; The MIS division may take over a user's account for troubleshooting purposes only, as it relates to the user's incident and/or circumstances. At such times, the user will be immediately notified, and a new/temporary password shall be issued to the user to ensure his/her ability to re-login into the system;
21. Unauthorized access to any of the DOF IT resources is strictly prohibited; users shall not attempt to gain excess, or go beyond their authorized, permissions. This includes attempting to log in through another user's or system's account or accessing/ attempting to access files without authorization. Unauthorized access is illegal; and
22. Immediate notification must be given to the supervisor, Finance Commissioner, Personnel Director or other administrator, or the MIS Director, once a user identifies a possible security breach of any sort.

c. Privacy and Safety

23. Users shall not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language on-line;
24. Users shall not post information that, if acted upon, could cause damage or endanger or disrupt normal business operations;
25. Users shall not engage in personal attacks, including prejudicial or discriminatory attacks while utilizing DOF IT resources, nor shall they harass other individuals via e-mail, instant messaging, or any other network/communications protocol;
26. Users shall not knowingly or recklessly post false or defamatory information about a person or organization;
27. Users shall not post personal contact information about anyone, for any purpose other than that which is to satisfy DOF systems requirements;
28. Users shall promptly disclose to a supervisor or other administrator of DOF's MIS division any message they receive that is inappropriate, offensive, or otherwise objectionable; and
29. Users may not use the DOF system to engage in partisan political activities, nor shall they make use of DOF IT resources to conduct personal business activities unrelated to the mission of the department.

d. E-mail & Internet Use

Use of e-mail services is a privilege, which imposes certain responsibilities and obligations on users. Transmission of e-mail to locations outside of the agency's local area network may require the use of the Internet for transport. Since the Internet and its tools adhere to open and documented standards and specifications, it is inherently an unsecured network that has no built-in security controls.

Connections to internet resources are vulnerable, and may expose the workstations, servers and the network to imminent internet threats such as viruses – hoaxes (such as phishing scams) and Trojan horses, spyware and malware. These are malicious software programs that can conveniently attach themselves to workstations and servers to destroy sensitive data.

30. Telnet and File Transfer Protocol (FTP) connections are allowed only to selective servers for specific purposes only; users requiring the use of these protocols must make written requests, will be advised by MIS accordingly. Only secure and authorized file transfers are allowed on the ERP and FMS;
31. Internet services are intended for periodic, active use of e-mail, newsgroups, file transfers, and browsing the internet. Authorized users may stay connected as long as is necessary for work related purposes only;
32. Internet chat, games and jest-full communications will not be tolerated; DOF's network is intended for government business only;
33. Spamming is not allowed on any DOF IT resource. Spamming is simultaneously sending an annoying or unnecessary message to a large number of people for purposes not relating to the government's financial operations;

34. E-mail communications, if allowed to accumulate on a server, can quickly consume the server's disk space and may cause system problems. Thus, users should check their e-mail frequently and delete unwanted messages promptly. The e-mail system is set up to automatically retain all incoming messages. All messages may be maintained by DOF indefinitely;
35. Users should use the e-mail system only as a transport and not as a repository for storing e-mail messages. E-mails that are required to be filed should be saved electronically outside the e-mail system;
36. The content of anything exchanged (sent and/or received) via e-mail communications must be appropriate and consistent with agency policy, subject to the same restrictions as any other correspondence;
37. Users shall take all reasonable precautions, to prevent the use of their e-mail account by unauthorized individuals; and
38. Modifying or attempting to alter e-mail headers will not be tolerated and is prohibited.

DOF also reserves the right to update, modify or alter this policy document as necessary without prior notice.

e. Data Breach

A data breach is an incident where confidential or protected information is accessed/retrieved without authorization of the system's owner. A data breach is recognized as a potential costly security failure of an organization. Technology alone cannot provide adequate security defense, as employees must be trained to avoid common security threats.

Security Awareness training is now offered for all DOF employees by the Bureau of Information Technology (BIT) on a quarterly basis.

Confidential data used for operational purposes relate to job applicants, current and former employees, payroll details, contracts, vendors' details, financial details.

Causes: Data breaches may be caused by employees, parties external to the organization or computer system errors.

***Human Error* –** Human error causes include:

- Loss of computing devices (portable or otherwise), data storage devices or paper records containing confidential data;
- Disclosing data to a wrong recipient;
- Handling data in an unauthorized way, e.g. downloading a local copy of confidential data;
- Unauthorized access or disclosure of confidential data by employees, e.g. sharing a login; and
- Improper disposal of confidential data, e.g. hard disk, storage media or paper documents containing confidential data sold or discarded before data is properly deleted.

***Malicious Activities* –** Malicious causes include:

- Hacking incidents, illegal access to systems/files containing confidential data; and
- Theft of computing devices (portable or otherwise), data storage devices or paper records containing personal data.

6.2 DUE PROCESS

In the event there is an allegation that a user has violated the acceptable use or the provisions of this *Information Technology Resource Regulation* policy, the user will be provided with a written notice of the alleged violation, and his/her account privileges may be suspended immediately. The user will be given an opportunity to present an explanation to a due process council for a final determination regarding continuing access to the system. Disciplinary actions will be tailored to meet the specific concerns related to the violation and to assist the user in gaining the self-discipline necessary to behave appropriately when dealing with the financial system, and/or the electronic network. Violations of the *Acceptable Use Policy* and the provisions of this regulation may be subject to disciplinary action up to and including immediate suspension of access privileges to the system, or dismissal, depending upon the nature of the violation, and may be subject to legal prosecution. Non-employees violating the *Acceptable Use Policy* and the provisions of this regulation shall have their access privileges immediately suspended and shall be subject to legal action and prosecution. Finance will cooperate fully with local, state and federal officials in any investigation concerning or relating to any illegal activities conducted through the DOF's systems.

System users have no right of privacy regarding materials sent, received or stored in any electronic data systems of Finance. Department officials reserve the right to review workstations and servers at any time to determine if such use meets the criteria set forth by the Department. If routine maintenance and monitoring of the system lead to the discovery that the user has or is violating the *Acceptable Use Policy* and this regulation, then an individual search will be conducted. The nature of the search/investigation will be reasonable in keeping with the nature of the alleged misconduct.

Users should be aware that their personal files may be subject to public inspection and copying under the legal statutes.

6.3 SERVICES PROVIDED

The Management Information Systems (MIS) division at Finance shall serve as the administrator with oversight of all the Department's IT systems. This division shall be responsible for, among other things, final approval and establishing employee, and other users accounts, setting quotas and retention schedule for disk usage on the system, establishing a policy on software installations, upgrades, systems maintenance and virus protection, and ensuring that processes are in place to satisfy system safety, accessibility, and data integrity, and enforce proper use of the Department's IT resources.

The ERP System provides financial information in the following modules or sub-systems: Budget, General Ledger, Requisitioning, Purchasing, and Accounts Payable, Cash Receipts, Payroll/Human Resources, and Fixed Assets. Ownership/management of system modules are as follows:

- Budget Administration - Office of Management and Budget
- General Ledger - Department of Finance
- Cash Receipts (A/R) - Department of Finance
- Purchasing - Department of Property and Procurement
- Accounts Payable - Department of Finance
- Human Resources - Division of Personnel
- Payroll - Department of Finance
- Fixed Assets - Finance and Department of Property and Procurement
- Grants/Project Management - Office of Management and Budget
- Vendor Self Service - Finance and Property and Procurement
- Employee Self Service Division of Personnel

Modules/functions not listed above remain under management and administration of the Department of Finance.

The STATS system is a resource to manage and administer employee time and attendance, and scheduling. The STATS system is centrally managed at the Department of Finance, and departments and agencies are allowed to administer selective system tasks pertaining to their employees for time and attendance reporting and payroll processing,

As the ERP system is designed for distributed processing, departments/agencies are responsible for initial annual budget entry, general ledger accounts reconciliation, requisitioning, accounts payable (A/P) invoice processing, cash receipting, and initialization of personnel actions processing. All non-distributed tasks will be performed by the department/agency with responsibility for that module. Policy and processing for administering most ERP tasks are available on-line at https://dof.vi.gov/resources/visionerp.

Reports and Printing Operations:

Departments are responsible for the generation of their own reports; where technical support is required, DOF will assist.

Technical Services:

Technical tasks necessary for up-keeping and fine-tuning of the system shall be completed at the discretion of MIS Division. To minimize interference with, or minimize impact on, daily operations, MIS will handle all major installations and configurations of the ERP software outside of regular business hours, generally with prior notice. All required end user software installations shall be the responsibility of the department/agency. Technical documentation for end user software installations to support ERP functionality is available on-line, at https://dof.vi.gov/resources/visionerp.

Internet and E-Mail:

Email is provided by Bureau of Information Technology (BIT). Internet service is provided by our Internet Service Provider (ISP). The Internet provides access to a wide range of information in the form of text, graphics, photographs, video and sound. E-mail will allow account holders to communicate with others within and outside the department. The use of these resources at the Department of Finance is restricted to Finance personnel only.

6.4 CONTACTING DEPARTMENT OF FINANCE

As custodians for the ERP system, the Department of Finance can be contacted as follows:

Department of Finance
2314 Kronprindsens Gade
Charlotte Amalie
St. Thomas USVI 00802
Telephone: (340) 774-4750
Facsimile: (340) 774-4028
https://dof.vi.gov/

Department of Finance
4008 Estate Diamond, Lot 7B
Christiansted
St. Croix USVI 00820
Telephone: (340) 773-1105
Facsimile: (340) 778-5002

Department of Finance Helpdesk can be reached as follows:

Telephone: (340) 774-4750, ext. 2121 or (340) 773.1105;
Facsimile: (340) 714-9442;
E-mail: dofhelpdesk@dof.vi.gov

Section 7. PROCEDURES:

MIS provides system access as authorized by D&As management. In accordance with Section 6, Policy, by participating in the use of the electronic network and systems provided by Virgin Islands Department of Finance (DOF), users agree to comply with policies governing their usage.

Section 8. COMPLIANCE AND ACCOUNTABILITY:

MIS shall enforce proper use of the Department's IT resources. As indicated in section 6.2 Due Process, if a user allegedly violates the acceptable use or the provisions of this policy, the user will be provided with a written notice of the alleged violation, and his/her account privileges may be suspended immediately. Violations may result in disciplinary action up to and including immediate suspension of access privileges to the system, or dismissal, depending upon the nature of the violation, and may be subject to legal prosecution. The Virgin Islands Department of Finance reserves the right to withdraw access to any user for violating the policies as described herein.

Section 9. APPENDICES:

Regulations/Examples

None.

Section 10. REVISION HISTORY:

Revision #	Date Requested	Author (Name/Title)	Description of Changes	Approved By (Name & Title)	Signature	Date Approved
0	07/01/2007	Alvin Williams	Initial Draft	Valdemier Collens, Finance Commissioner	VC	04/01/2023
1	10/23/2025	Kerry Henry	Revisions Reviewed / Approved	Kevin McCurdy, Finance Commissioner	KM 	10/30/2025