



1.0 PURPOSE

The purpose of this Procedure is to specify the process for State agencies when requesting an investigation into any State employee's technology-based activity. **This procedure should not be construed to convey any expectation of privacy.**

2.0 SCOPE

This procedure applies to all Departments (including agencies, boards, and commissions) within the Executive Branch of West Virginia State Government, excluding constitutional officers, the West Virginia Board of Education, the West Virginia Department of Education, and the county boards of education. However, the West Virginia Office of Technology (WVOT) recommends that all Agencies, including those excluded above, follow this procedure.

Supervisors and managers must follow this procedure to initiate investigations of persons using State equipment and systems.

3.0 REQUIREMENTS

- 3.1 To gain access to information about employees' technology-based activities, a suspected violation of law or policy should be identified to initiate the required technical investigations.
- 3.2 Any supervisor or manager may initiate a **request** for access. However, only Office Directors, Commissioners, Cabinet Secretaries, or the *Legislature's Commission on Special Investigations have the authority to **approve and submit** requests for investigations of staff in their **own** office, agency, or department. (**may request from any office*)
- 3.3 Agencies should exercise discretion when requesting reports of user activities, and should involve both Agency Legal and Personnel services in the decision to submit such requests.
- 3.4 The Service Desk, or any WVOT employee, must immediately transfer all investigation requests to the Office of Information Security and Controls (OISC).
- 3.5 All employees involved in technical investigations are required to keep all information discovered in the process confidential.

For Internal
State Use Only

Procedure: Technical Investigation Request

State of West Virginia Office of Technology

Policy No: WVOT-PR1001

Issue Date: 02/26/08

Revised: 9/1/2016

Page 2 of 7

4.0 PROCEDURE

- 4.1 ALL investigation requests must be submitted to WVOT through electronic form found at SOCFORMS.WV.GOV.
- 4.1.1 If an agency or organization is not on the state network or unable to use the website, the requester may use the form in Attachment B of this document.
- 4.2 When requesting a technology-related investigation for any State employee the following information must be submitted at SOCFORMS.WV.GOV:
- 4.2.1 Name, title, agency name, and phone number of the supervisor or manager requesting the investigation;
- 4.2.2 Name, e-mail address, and userid of the individual whose activity will be investigated;
- 4.2.3 Purpose of Investigation or Suspected Violation (ex: to confirm suspicion of abuse or misuse; to remove cloud of suspicion, to validate user presence, etc.) As a guide to the kinds of violations that merit investigation, examples include, but are not limited to the following:
- 4.2.3.1 Suspected violations of the law. Examples include, but may not be limited to the following:
- Criminal enterprise;
 - Sexual harassment; and
 - Willful misuse of legally protected information, etc.
- 4.2.3.2 Suspected violations of State policy. Examples include, but may not be limited to the following (For more information, see "Appendix A" of WVOT-PO1001 - *West Virginia State Information Security Policy*):
- Determination of excessive personal use;
 - Commercial enterprise purposes or for-profit activities;
 - Sexually explicit use;
 - Chain letters;
 - Behaviors that introduce viruses or other malware;
 - Disabling security systems or controls; and
 - Breach of confidentiality, unethical conduct.

FOR

Procedure: Technical Investigation Request

State of West Virginia Office of Technology

Policy No: WVOT-PR1001

Issue Date: 02/26/08

Revised: 9/1/2016

Page 3 of 7

- 4.2.4 Interval of Investigation (ex: 03/01/06 to 08/15/06); and
- 4.2.5 Report Due Date (based upon urgency).
- 4.3 If it becomes necessary to expedite the delivery of a request, the Chief Information Security Officer (CISO) or, if the CISO is unavailable, the Chief Technology Officer (CTO) should be contacted for immediate assistance.
- 4.4 The CISO will work with other Directors as needed to assign investigative tasks to the appropriate technicians.
- 4.5 The WVOT will perform a best-effort investigation over the specified interval to determine the existence of findings that could indicate a violation. The authorized requestor agrees to the following:
- 4.5.1 The WVOT may utilize any sources, tools, or technologies needed to provide the most accurate, detailed, and relevant information possible;
- 4.5.2 The individual under investigation will remain separated from the investigator at all times; and
- 4.5.3 All acquired materials and data gathered will remain in the custody of the investigator. Materials may be acquired in two ways:
- Remotely (requires chain of custody form)
 - On-Site
- 4.6 The CISO will send the authorized requestor a detailed report of the findings resulting from the investigation. This will follow the same path as the request (technician –CISO– requestor). A copy of the report may (when warranted) also be forwarded to the Agency Personnel Office and the West Virginia Division of Personnel. Criminal activity findings may be reported directly to law enforcement.
- 4.7 Agencies using investigative services provided by the WVOT may be billed according to a standard rate structure.

5.0 ENFORCEMENT

Not applicable to this document

6.0 DEFINITIONS

- 6.1 Cabinet Secretary – The leader of a Department appointed by the Governor.

Procedure: Technical Investigation Request

State of West Virginia Office of Technology

Policy No: WVOT-PR1001

Issue Date: 02/26/08

Revised: 9/1/2016

Page 4 of 7

- 6.2 Chief Information Security Officer (CISO) - Person designated by the CTO to oversee Information Security practices and initiatives for the Executive Branch of WV State government, excluding the constitutional officers.
- 6.3 Chief Technology Officer (CTO) – The person responsible for the State’s information resources.
- 6.4 Commissioner - The leader of a State organizational entity (Bureau, Commission, etc.)
- 6.5 Contractor – Anyone who has a contract with the State or one of its entities.
- 6.6 E-mail – Any message sent electronically through one or more computers and/or communications networks, and in most cases has a human originator and receiver.
- 6.7 Employee – Individuals retained and authorized on a temporary or permanent basis by the State of West Virginia to perform a service. For the purposes of Information Technology and Security policy, the term “employee” shall include the following: contractors, subcontractors, contractors’ employees, volunteers, county health department staff, business associates, and any other persons who are determined and notified by the WVOT to be subject to this policy. This definition does not create any additional rights or duties.
- 6.8 Legislature’s Commission on Special Investigations – The group charged with performing a range of investigative tasks, including suspected purchasing violations, illegal conduct by State employees, conflicts of interest, bribery of State officials, and malfeasance. This body may also recommend action to the Attorney General, prosecuting attorney, or other authority empowered to act upon such recommendation. (See http://www.legis.state.wv.us/Joint/Special_Investigations/csi_mission.cfm)
- 6.9 Malware - Software designed to infiltrate or damage a computer system without the owner's informed consent. It is a blend of the words "malicious" and "software". The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.
- 6.10 Office Director – The designated or appointed leader of a state organizational entity who generally reports directly to the head of the agency, such as a Commissioner.

FOR

Procedure: Technical Investigation Request

State of West Virginia Office of Technology

Policy No: WVOT-PR1001

Issue Date: 02/26/08

Revised: 9/1/2016

Page 5 of 7

- 6.11 Office of Information Security and Controls (OISC) - The functional unit charged with the responsibility to undertake and sustain initiatives to promote, enhance, monitor, and govern actions, standards, and activities necessary to safeguard data and information systems within the Executive Branch of WV, as provided in West Virginia Code §5A-6-4a and the Governor's Executive Order No. 6-06.
- 6.12 Procedure – A series of steps followed in a definite regular order ensuring the consistent and repetitive approach to actions.
- 6.13 Userid – A unique “name” by which each user is identified to a computer system.
- 6.14 West Virginia Division of Personnel – The Division of the Department of Administration established by WV CODE § 29-6-1 *et seq.*, which is responsible for the system of human resource management for operating agencies in the classified and classified-exempt service of West Virginia State government.
- 6.15 West Virginia Office of Technology (WVOT) - The division of the Department of Administration established by WV Code § 5A-6-4a, *et. seq.*, which is led by the State’s CTO and designated to acquire, operate, and maintain the State’s technology infrastructure. The WVOT is responsible for evaluating equipment and services, and reviewing information technology contracts.

7.0 Change Log History

- January 30, 2015 – Added Change Log History
- 9/1/2016 – Policy Reviewed. No edits made.

FOR



Appendix A: SOCFORM.WV.GOV INSTRUCTIONS

Issued by the CTO

1. Open browser and go to socforms.wv.gov.
2. Click on **New Investigation**.
 - a. Enter your **wv.gov** email address in the **Supervisor Email** field.
 - b. After you enter your email address, hit **Tab** or click in the next field.
3. If you are in active directory, the page should automatically load your information
4. Fill in the rest of the Supervisor fields if needed.
5. If you are also an approval authority, you may click the **Authority is same as Supervisor** checkbox which will automatically copy your **Supervisor** information to the **Authority** fields.
6. After you fill that out, please fill in the information for the person to be investigated.
7. You will then enter the **PAS** number. You **MUST** enter a **PAS** number in order to submit the form.
8. Please select your department and agency. If your specific agency is not listed, please contact the Security Operations Center to add your agency.
9. Click **Next Step**.
10. On this page, please select the dates for investigation and fill out the Purpose of the investigation.
11. Determine if you need a web history investigation, email investigation, forensic hard-drive investigation, or a combination of any of those.
12. If there is any other information that you need to tell us, please fill out the **Other** field.
13. Click **Finish/Submit**.
14. You should receive a confirmation email to the email that you provided if the submission was successful.
15. An email will then be sent to the **Approval Authority** for authentication and approval.
16. Someone from the Security Operations Center will get in contact with you after receipt of the investigation form.



State of West Virginia Office of Technology Procedure:
Appendix B:
Technical Investigation Request Form
Issued by the CTO

Requesting Technical Investigation/Information
****Sections 1 through 3 must be filled out by Supervisors or Managers Only****

Section 1

- 1. Supervisor or Manager Requesting Investigation: _____
- 2. Title: _____ 3. Agency: _____
- 4. Phone # _____ 5. Email: _____
- 6. Billable PAS # _____

Section 2 (If a person is being investigated)

- 1. Name of Individual to be Investigated: _____
- 2. Email: _____ 3. UserID: _____

Section 3

- 1. Purpose of Investigation or Suspected Violation:
 (see 4.1.3 of WVOT-PR1001, attach additional pages if necessary to explain)

- 2. Interval of Investigation From: _____ To: _____

Section 4

This section must ONLY be filled out by a Cabinet Secretary, a Commissioner, an Office Director, the Office of Special Investigations, or an Equivalent Authority (e.g. GEIST Member):

- 1. Has the Technical Investigations procedure been read and understood? ___ Yes ___ No
- 2. Has the requestor provided sufficient information to initiate this investigation? ___ Yes ___ No
- 3. Does your Agency require Legal and/or Personnel approval for investigation actions? ___ Yes ___ No
- 4. If so, has this request been approved by your Agency Legal and/or Personnel Dept.? ___ Yes ___ No
- 5. (Print) Name: _____ 6. Title: _____
- 7. Agency: _____
- 8. Email: _____ 9. Phone: _____
- 10. Signature: _____ 11. Date: _____

This form must be forwarded to the Chief Information Security Officer (CISO) along with ALL supporting documentation. Send by Fax: 304-957-0137 OR Mail: West Virginia Office of Technology, Building 5, 10th Floor, 1900 Kanawha Blvd., Charleston, WV 25305, Attn: CISO