



DEPARTMENT OF ADMINISTRATION

Enterprise Policy

DOIT-10-08-2008

DIVISION OF INFORMATION TECHNOLOGY

Forensic Investigation and Authorization Policy

Date of Last Revision 09/03/2008

Bijay Kumar

(401) 574-9220

bijay.kumar@doit.ri.gov

1. Purpose

- a. The purpose of this document is to establish policy and procedure for requesting an investigation involving the use of computers and/or any other devices capable of storing electronic data.
- b. A process should be established for dealing with incidents that require non-criminal forensic investigation. This policy is not meant to supersede any standards of best practice for criminal forensic investigations.

2. Applicability

- a. This policy is applicable to all persons who may request computer forensic services from the RI Division of Information Technology (DOIT) or perform computer forensic services on behalf of DOIT.

3. Objectives

- a. Establish the appropriate requirements for requesting an examination involving the use of computers and/or any other devices capable of storing electronic data.

4. Investigation Authorization Requests and Approvals

- a. The following State officials are authorized to approve/direct an investigation which involves the use/misuse of computers and any other related devices capable of storing electronic data
 - (i.) State Chief Information Officer (CIO) or designee;
 - (ii.) Agency HR representative;
 - (iii.) Agency Director's representative;
 - (iv.) State Chief Information Security Officer (CISO) or designee.
- b. An investigation request can be submitted by e-mail, letter, and/or fax using the "Authorization for Computer Forensic Services" form.
- c. Agency Information Manager (AIM) or Technical Support Manager (TSM) shall make his/her investigation request through his/her respective HR representative.

5. Forensic Investigation Process

- a. The scope of the forensic investigation will be determined by the State Computer Examiner assigned to the case.

- b. Physical chain of custody will be maintained at all times utilizing the "DOIT Chain of Custody Document".
- c. Updates and notifications on the forensic case will be provided to the requestor based on the progress as determined by the State Computer Examiner.
- d. Any copies of the forensic reports must be produced by DOIT and accompanied by the "DOIT Removable Media Transmittal Sheet"

6. State Computer Examiner Compliant Activities

- a. Examination of media should be conducted in a forensically sound examination environment;
- b. Properly prepared media should be used when making forensic copies to insure no commingling of data from different cases. Properly prepared media is that which has been completely overwritten and is in compliance with the DOIT Policy "Media Handling and Security" Policy #05-01. State Computer Examiner should always sterilize the media used for evidence acquisition and image storage with the Department of Defense compliant disk wiping utility.
- c. Verify successful acquisition by comparing known values of the original and the copy or by doing a sector-by-sector comparison of the original to the copy.

7. Exceptions to Policy

- a. Exceptions to this policy may be granted solely by the CISO or the CISO's designee.
- b. The examination may be performed by an approved outside entity at the discretion of the CISO or the CISO's designee.
- c. Examinations deemed criminal will be turned over to the appropriate law enforcement agency.

8. Implementation Responsibility

- a. Only State Computer Examiners can perform computer examinations in the State of Rhode Island and its agencies unless an exception has been provided.
- b. State Computer Examiners will follow all aspects of DOIT policies in computer forensics.

9. Compliance Responsibility

- a. The DOIT and the State Agencies shall be responsible for implementing and enforcing this policy within their supported areas.

10. Definitions

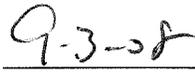
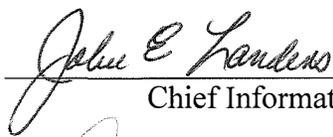
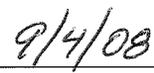
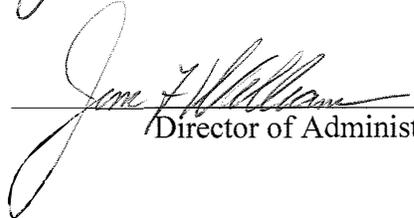
- a. **Computer Forensics** - The scientific examination and analysis of data held on, or retrieved from, computer storage media in such a way that the integrity of the information can be used as evidence in a court of law.
- b. **Computer Forensic Investigations (CFI)** - A scientific investigation involving acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media.

- c. **Media** - media including but not limited to hard drives, removable media (flash drives, floppy discs, CDs, DVDs, etc.), media from PDA and Blackberry devices.
- d. **Forensically-sterile media** - media properly wiped with the Department of Defense compliant utility at least 4 times (three overwrite passes and a full verification pass) and verified by the examiner.
- e. **Forensically sound examination environment** - is one which is completely under the control of the examiner: no actions are taken without the examiner permitting them to happen; and when the examiner permits or causes an action he/she can predict with reasonable certainty what the outcome of the action will be.
- f. **State Computer Examiner** - an investigator with specialized training in the area of computer forensics responsible for the recovery, analysis, and subsequent presentation of electronic evidence and authorized by the State CIO.
- g. **Forensic software** - properly licensed copy of the software used by the computer examiner.

11. Attachments

- a. Authorization for Computer Forensic Services Form
- b. DOIT Chain of Custody Document
- c. DOIT Removable Media Transmittal Sheet

12. Signatures

 <hr/> Chief Information Security Officer	 <hr/> Date
 <hr/> Chief Information Officer	 <hr/> Date
 <hr/> Director of Administration	 <hr/> Date

	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	10-08	Accepted		09/03/2008	5 of 12
State of Rhode Island Department of Administration Division of Information Technology		TITLE	Policy on Forensic Investigation and Authorization		
		DRAFTED BY	Dmitry Kuchynski		

Authorization for Computer Forensic Services

General Information (required)	
<input type="checkbox"/> Agency Official has been contacted: _____ <div style="text-align: right; font-size: small;"><i>Name of the Agency Official contacted</i></div>	
<input type="checkbox"/> This request has been evaluated / reported to the member of the legal department or State Police _____ <div style="text-align: right; font-size: small;"><i>Name and Title of Responsible person(s)</i></div>	
Name and Title of Person Requesting Forensics: <i>(results will be reported to this individual)</i>	
Address:	Contact Phone#:
Notes:	

Details on the case (required)
1. Why do you need this service? <ul style="list-style-type: none"> <input type="checkbox"/> To administer appropriate use audits <input type="checkbox"/> To assist in the investigation/prosecution of an employee <input type="checkbox"/> To assist in the investigation/prosecution of a customer <input type="checkbox"/> To gain access to an employee's encrypted or password protected data <input type="checkbox"/> To identify source of hacker/terrorist <input type="checkbox"/> To recover deleted data files <input type="checkbox"/> To recover reformatted drive data <input type="checkbox"/> Other
2. What kind of data are you seeking? <ul style="list-style-type: none"> <input type="checkbox"/> Employee Work Documents <input type="checkbox"/> Entire Drive recovery

	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	10-08				
State of Rhode Island Department of Administration Division of Information Technology		TITLE	<i>Policy on Forensic Investigation and Authorization</i>		
		DRAFTED BY	Dmitry Kuchynski		

- Harassment documentation
- Employee internet/email abuse
- Internal malicious data
- External malicious data
- Pornographic graphic files
- Illegal activity
- Other

3. If data may be taken to court, will case be:

- Civil
- Criminal
- Employment termination
- Other

Note: any criminal investigation needs to be forwarded to the RI State Police or FBI and will not be handled by DOIT

4. What kind of computer needs to be examined?

- Desktop computer
- Digital Camera
- Floppy Disk
- Laptop computer
- Memory card
- Workstation
- Zip disc

Other

5. How many computers need this service?

- 1
- 2
- 3-5
- more then 5

6. What is the Operating System?

- Windows 95/98/ME
- Windows 2000
- Windows NT
- Windows XP
- Windows 2003
- Other

7. Priority of the Case:

- Low
- Medium
- High

	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	10-08	Accepted		09/03/2008	7 of 12
State of Rhode Island Department of Administration Division of Information Technology		TITLE	<i>Policy on Forensic Investigation and Authorization</i>		
		DRAFTED BY	Dmitry Kuchynski		

Member of the agency management: _____ Date: _____

Member of the DOIT Security Management: _____ Date: _____

	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	10-08	Accepted		09/03/2008	8 of 12
State of Rhode Island Department of Administration Division of Information Technology		TITLE	<i>Policy on Forensic Investigation and Authorization</i>		
		DRAFTED BY	Dmitry Kuchynski		

DOIT Chain of Custody Document

Submitting Activity	
Before submitting any computer components, you must print and fill out by hand the Chain of Custody Form. The purpose of the document is to prove that the integrity of the evidence was maintained through seizure to the production to court if necessary.	
<input type="checkbox"/> Agency Official has been contacted: _____ <div style="text-align: center; font-size: small;"><i>Name of the Agency Official contacted</i></div>	
<input type="checkbox"/> Name and title of person from whom received (owner, other _____) <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> <div style="text-align: center; font-size: small;"><i>Name and Title of Responsible person(s)</i></div>	
Name and Title of Person Requesting Forensics: <i>(results will be reported to this individual)</i>	
Address:	Contact Phone#:
Location from Where Obtained:	
Description of Item to Be Tested:	Date Obtained:
Name and Title of Person Collecting Evidence: <i>(if different from above)</i>	Time Obtained:

For Internal Use Only

Article Received from: *(name, title, federal express package, etc)*

Description of Articles

	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	10-08	Accepted		09/03/2008	11 of 12
State of Rhode Island Department of Administration Division of Information Technology		TITLE	<i>Policy on Forensic Investigation and Authorization</i>		
		DRAFTED BY	Dmitry Kuchynski		

DOIT ENTERPRISE SECURITY

DOIT Removable Media Transmittal Sheet

Date:

Case:

Number of media items (for ex. CDs):

Description of Contents:

Transmitted by:

Name: _____

Signature: _____

Received by:

Name: _____

Signature: _____

	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	10-08	Accepted		09/03/2008	12 of 12
State of Rhode Island Department of Administration Division of Information Technology		TITLE	<i>Policy on Forensic Investigation and Authorization</i>		
		DRAFTED BY	Dmitry Kuchynski		

****NOTE**** Please request any required duplicates of removable media from DoIT Security. **Do Not** make duplicates of the media.