



**Maine State Government
Dept. of Administrative & Financial Services
Office of Information Technology (OIT)**

Forensic Investigation Workflow Policy

1.0 Statement

The Office of Information Technology (OIT) follows a well-defined workflow to perform *forensic*¹ investigations.

2.0 Purpose

The purpose of this policy is to codify an effective, efficient, and discreet workflow to perform forensic investigations.

3.0 Applicability

This policy applies to all forensic investigations conducted by OIT.

4.0 Responsibilities

- 4.1 Chief Information Officer (CIO): The Chief Information Officer owns and enforces this policy.
- 4.2 DAFS-Bureau of Employee Relations (BER): Within DAFS-BER, a forensic investigation can be requested only by the State EEO Coordinator.
- 4.3 DAFS-Bureau of Human Resources (BHR): Within DAFS-BHR, a forensic investigation can be requested only by a person in the rank of HR Director or above.
- 4.4 Legislative, Judicial or Constitutional Branches: Within these Branches, a forensic investigation can be requested only by the HR Director.
- 4.5 Office of the Attorney General (AG): Within the Office of the AG, a forensic investigation can be requested only by a person in the rank of Assistant Attorney General (AAG) or above.
- 4.6 OIT Technical Staff: OIT Technical Staff execute this policy.

5.0 Directives

- 5.1 OIT Technical Staff take delivery of the *evidence*² or investigation request exclusively from

¹ Forensic- Scientific tests or techniques used in connection with the detection of crime.

² Evidence- Any I.T. asset or data that is the subject of forensic investigation. I.T. assets include, but are not limited to, workstations, desktops, laptops, external drives, compact discs, digital video discs, universal serial bus memory sticks, or any other removable media. Data includes, but is not limited to e-mail, stored documents, and website visit logs. In forensic computer investigations of criminal matters, evidence may also include a duplicate image of the device to conduct the investigation so as not to corrupt the original.

Forensic Investigation Workflow Policy

the *Requester*³. OIT Technical Staff never take delivery of the evidence or request from the *User*⁴.

- 5.2 Once OIT Technical Staff take delivery of the evidence or request, OIT maintains strict *Chain-of-Custody*⁵ of the evidence or any data related to the investigation through the forensic investigation, until OIT delivers the evidence or data back to the Requester.
- 5.3 OIT Technical Staff *never* communicate with the User. All communication from OIT is addressed exclusively to the Requester.
- 5.4 OIT Technical Staff *always* provide a written report to the Requester, describing the results of the forensic investigation.
- 5.5 OIT Technical Staff treat any and all forensic investigations on a need-to-know basis. Any HR investigation is considered CONFIDENTIAL. A Footprints ticket titled HR Investigation may be created for all investigations, so that OIT Technical Staff time can be tracked. However, if a ticket is created, the ticket creator and anyone updating the ticket **MUST** ensure that no personally identifiable information about the User is entered into the ticket. If it appears laws may have been broken, Law Enforcement will be consulted.
- 5.6 OIT Technical Staff maintain several confidential Standard Operating Procedures that specify in great detail the exact steps undertaken to support this policy.

6.0 Document Information

Initial Issue Date: February 7, 2013

Latest Revision Date: January 23, 2017 – to update Document Information.

Point of Contact: Architecture-Policy Administrator, OIT, Enterprise.Architect@Maine.Gov

Approved By: Chief Information Officer, OIT

Legal Citation: [Title 5, Chapter 163: Office of Information Technology](#)⁶.

Waiver Process: See the [Waiver Policy](#)⁷.

³ Requester: An authorized individual (e.g. HR Director, AAG, State EEO Coordinator), who requests the forensic investigation.

⁴ User: The State personnel who is subject to the investigation or who uses the I.T. asset that is the subject of the forensic investigation.

⁵ Chain-of-Custody: Documented audit trail verifying the receipt, custody, handling, control, transfer, and disposition of evidence in a manner to avoid possibility of tampering or misconduct.

⁶ <http://legislature.maine.gov/statutes/5/title5ch163sec0.html>

⁷ <http://www.maine.gov/oit/policies/waiver.htm>