**Information Technology Supporting Documentation**
**Commonwealth of Pennsylvania**
**Governor's Office of Administration/Office for Information Technology**

| | | |
|---|---|---|
| **Document Number:** | **OPD-PRV002A** | |
| **Document Title:** | **Privacy Officer Escalation Procedures** | |
| **Issued by:** | **Deputy Secretary for Information Technology** | |
| **Date Issued: February 16, 2006** | | **Date Revised: November 18, 2010** |
| | | |
| **Domain:** | **Privacy** | |
| **Discipline:** | **Privacy** | |
| **Technology Area:** | **Compliance** | |
| **Referenced by:** | **ITP-PRV002** | |
| | | |
| **Revision History Date:** | **Description:** | |
| **11/18/2010** | **ITP Refresh** | |

The privacy officer (PO) appointed for each agency is responsible for enforcing the *Commonwealth Electronic Information Privacy Policy* specific to his/her agency as defined in ITP-PRV001.

Areas subject to enforcement:

- **E-government Web sites –** Outlines standards for agency e-government Web sites and applications with respect to privacy considerations;
- **Agency Electronic Information Confidentiality Agreement/Statement –** Provides guidance for the creation and enforcement of agency *Electronic Information Confidentiality Statements*; and
- **Creating/Maintaining Auditable Data –** Provides guidance for categorization of data and user types for authentication and access logging for use in audits.

If the PO determines that his/her agency is not in continuous compliance with the standards set forth in ITP-PRV001, the PO may utilize the following escalation checklist. This list may include steps outside of the PO's normal chain of command.

**Escalation Procedures:**
The following procedures should be used for escalation of agency privacy compliance issues:

1. The agency PO determines that the agency is not in continuous compliance with any aspect of ITP-PRV001.
2. The agency PO provides written notification of the issue to the agency chief information officer (CIO), chief information security officer (CISO), and any other personnel deemed appropriate. If an immediate solution to the issue can be identified, then the issue is resolved.
3. If an immediate resolution cannot be reached, the agency PO will schedule a meeting with all pertinent parties within two weeks of notification about the issue.
4. If the agency PO is unable to schedule this meeting due to lack of response from pertinent parties, the PO will notify, in writing, the Office of Administration privacy officer (OA/PO) about the issue (see *OA Notification* section).
5. In the scheduled meeting the group will determine a projected deadline and a remediation plan based upon the severity of the noncompliance.
6. The agency PO will monitor agency progress against the remediation plan and projected deadline.
7. If the remediation plan is successfully completed, the issue is resolved.
8. If the projected deadline is not achieved, at the PO's discretion, the agency PO will notify, in writing, the OA/PO about the issue (see *OA Notification* section).



Predefined supplemental document type codes are listed below:
**APP** = Appendix **BPD** = Best Practice Document **GEN** = General Information Document
**OPD** = Operations Document **RFD** = Existing Supporting Document Referenced by this ITP **WHP** = White Paper

9. If the agency is making efforts toward the corrective action and a reasonable modified deadline is created, the PO is not required to notify the OA/PO unless otherwise directed by the OA/PO.
10. If notified by the Agency PO of an issue, the OA/PO will monitor agency progress against the revised remediation plan and projected deadline(s).
11. If the subsequent deadline(s) are missed, the OA/PO will notify, in writing, the chief technology officer (CTO) and the deputy chief information officer (DCIO) of policy infringements and these entities will determine actions to be taken.

**OA Notification**

The OA/PO will notify in writing, and schedule a meeting with the agency PO and CIO, the CTO, and the DCIO for the Community of Practice in which the agency participates, as appropriate, upon escalation of an issue by an agency PO. This meeting will establish responsible parties, next steps, and deadlines.

**When to Escalate an Issue**

The PO may escalate a privacy issue in the following situations:

1. The agency does not meet and/or enforce applicable federal, state, and other mandates specific to electronic information privacy, provided the PO discusses the situation with Agency Legal Counsel prior to escalation;
2. The agency has not completed the reporting responsibilities to OA/OIT regarding the agency's compliance with ITP-PRV001;
3. The agency does not categorize electronic information and users in accordance with ITP-PRV001;
4. The agency does not distribute and maintain an agency electronic information confidentiality agreement; or
5. The agency does not comply with ITP-PRV001 in any other areas identified by the PO.

**Information to Include in Notification**

Notification to the OA/PO must be in writing and should include the following:

1. A description of the non-compliance issue, including, as appropriate, the system(s), statutory obligations, etc.;
2. A description of actions, if any, taken-to-date to attempt to correct the issue.

**Acronyms**

CIO - Agency Chief Information Officer
CISO - Agency Chief Information Security Officer
COP - Community of Practice
CoPA - Commonwealth of Pennsylvania
CTO - Office of Administration Chief Technology Officer
DCIO - Office of Administration Deputy Chief Information Officer
OA/PO - Office of Administration Privacy Officer
PO - Agency Privacy Officer