

## Privacy Management Annual Audit Plan

---

The ORL Privacy Officer will monitor, audit, and revise the effectiveness of program controls where necessary. This process will include:

- a) **Monitoring and updating the personal information inventory** continuously to keep it current and identify and evaluate new collections, uses, and disclosures.
- b) **Reviewing and updating policies** as needed following assessments or audits, in response to a breach or complaint, new guidance, industry-based best practices, or as a result of environmental scans.
- c) **Reviewing and updating privacy impact assessments and security threat and risk assessments as evergreen documents**, so that the privacy and security risks of changes or new initiatives within the organization are always identified and addressed.
- d) **Reviewing and updating training and education** on a periodic basis as a result of ongoing assessments and communicate changes made to program controls.
- e) **Reviewing and updating breach and incident management response protocols** to implement best practices or recommendations and lessons learned from post-incident reviews.
- f) **Reviewing and updating requirements in contracts** with service providers.
- g) **Reviewing and updating external communication** explaining privacy policies.

The Privacy Officer will review the following:

- The latest threats and risks.
- Program controls addressing new threats and reflecting the latest complaint or audit findings, or guidance of the Registrar.
- New services being offered that involve increased collection, use, or disclosure of personal information.
- Training, policies and procedures.

If the monitoring process uncovers a problem, the appropriate official will document and address concerns.

## **Information Systems**

The Privacy Officer will also review the controls the IT department has in place for systems that contain personal information. The Privacy Officer will review the following checklist once a year.

### **IT Security Audit Program**

- All relevant statutory, regulatory, and contractual requirements explicitly defined and documented for each information system.
- All system/audit logs that relate to the handling of personal information: Securely and remotely logged to a read-only medium that has an alert system when tampering is attempted.
- All system/audit logs that relate to the handling of personal information: Regularly monitored.

### **Ongoing Audits**

- Procedures in place to ensure that security events (e.g. unauthorized access, unsuccessful system access attempts, etc.) are identified, recorded, reviewed, and responded to promptly.
- Proactive audits conducted at regular intervals to verify the logical and physical consistency of the data, in order to identify discrepancies such as lost records, open chains, incomplete sets and improper usage.
- Active monitoring in place to ensure that personal information cannot be passed between computers, or between discrete systems within the same computer, without authority.

### **Scheduled Audits**

- Software/hardware inventory maintained and up-to-date.
- Annual physical inventory of all storage media containing personal information and discrepancies investigated immediately and corrected.

### **Audit Verification**

- Audit monitoring and review procedures to promptly detect errors in procedures and results.

## **Audit Implementation**

- Management personnel responsible for the audited area oversee the implementation of audit recommendations, verify completion of implementation and report verification results.