Name of Policy: Compliance incident reporting **Policy Number**: 3364-15-03 **Approving Officer**: President **Responsible Agent**: Director of Internal Audit and Chief Compliance Officer **Scope**: All University of Toledo Campuses			**Revision date:** June 1, 2016 **Effective date**: August 1, 2008
	New policy proposal	X	Minor/technical revision of existing
	Major revision of existing policy		Reaffirmation of existing policy

(A) Policy statement

The university strives to comply with all federal, state, and local statutes. This policy sets forth the procedures that the University of Toledo will use to respond to reports by institutional members or others regarding possible violations of university policies and procedures or a possible violation of applicable state and federal laws.

The following list includes, but is not limited to, critical areas of compliance:

(1) Fraud and abuse/false claims
(2) Research
(3) Construction
(4) Family educational rights and privacy act ("FERPA")
(5) Health insurance portability and accountability act ("HIPAA")
(6) National collegiate athletic association ("NCAA")
(7) Record industry association of America ("RIAA")
(8) Public records laws
(9) Ohio ethics laws
(10) Discrimination laws
(11) Federal financial aid
(12) Medicare and Medicaid anti-kickback statutes/stark laws
(13) Improper claims for clinical trials/provider based clinics/organ acquisition
(14) Direct graduate medical education/indirect medical education

(DGME/IME) reimbursement
(15) Emergency medical treatment and active labor act ("EMTALA")
(16) Medicare part D
(17) Joint commission
(18) University and medical center policies

(B) Purpose of policy

(1) This policy establishes the university's response in situations where:

(a) The policies, rules and standards of the university may not have been followed;

(b) Individuals may have knowingly or inadvertently violated university policies, rules and standards or applicable state or federal regulations;

(c) Corrective action or procedures are necessary to be compliant with university policies, rules or standards or applicable state or federal regulations;

(d) It is necessary to protect the university in the event of civil or criminal enforcement actions;

(e) It is necessary to preserve and protect the university's assets.

(C) Definitions

(1) Availability. Assurance that information, the computing systems used to process the information, and the security controls used to protect the information are all available and functioning correctly when the information is requested.

(2) Confidentiality. Assurance that information is accessible only to those authorized to have access.

(3) Incident. Any time that sensitive information, is viewed, accessed or attempted to be accessed, discussed, communicated

outside of the normal treatment, payment, or other normal operations of the university. An incident is also considered an action that compromises information, the access to information, or the integrity of our information infrastructure.

Below is a listing of incident examples. This list is not inclusive, and serves as a guideline.

(a) Disclosing or transmitting sensitive information when authorization has not been granted;

(b) Accessing information for which you have not been approved for or using resources for anything outside of your required job functions;

(c) Using sensitive information on another's behalf without consent;

(d) Speaking or displaying sensitive information in close proximity of others without consideration of privacy or confidentiality;

(e) Stealing information or physical assets;

(f) Recognizing any behavior or characteristic that doesn't "seem right";

(g) Using equipment that is not authorized for campus usage or is illegally obtained;

(h) Using sensitive information to maliciously cause harm.

(4) Institutional members. Anyone who participates in university activities, or has an affiliation with The University of Toledo; includes, but is not limited to general staff, managers, medical staff, contractors, vendors, students, alumni and others involved in treatment, payment, or other normal operations of the university, whether or not they are paid by the university.

(5) Integrity. Assurance that information has not been modified or destroyed in an unauthorized manner

(6) Whistleblower. A whistleblower is an institutional member who reports misconduct to people or entities that have the power to take corrective action.

(D) Procedures related to incident reporting

(1) Institutional member duty.

Institutional members have a duty to ask questions regarding potential issues and to report potential concerns. If any institutional member knows of or suspects a violation, they are to report it immediately without fear of retaliation. At no time will any retaliatory action be taken against any individual who files a complaint. Refer to the university's Non Retaliation policy 3364-15-04.

(2) Reporting methods.

To respond to these concerns, the university has established the following channels for institutional members to report incidents or other suspicious activities. Information collected during the reporting process will only be used to complete investigation into the reported incident, while maintaining confidentiality and privacy to the extent the law permits.

(a) Local resolution.

The recommended method to raise a concern begins with your own college, department or unit through supervisory channels.

(b) Central offices.

Due to the subject matter, work or personal relationship, it may be best to raise questions through a specialized central office. Examples include:

(i) Human resource office or the office of institutional diversity for concerns regarding discrimination or sexual harassment;

(ii) Athletic compliance officer for possible NCAA violations;

(iii) Research compliance officer for research concerns.

(c) Internal audit and compliance department.

If the institutional member is uncomfortable with addressing concerns at the local level or through a central office, needs advice on how to handle an issue, or issues have not been resolved satisfactorily, the institutional member can call and report directly to the internal audit and compliance department. Institutional members may also submit a written report to the internal audit and compliance department. Alternately, institutional members may also contact the Director of Internal Audit and Chief Compliance Officer directly at 419-530-8718.

(d) Anonymous reporting line.

The university has an anonymous reporting line to report any situation without using any personally identifiable information (888-416-1308). Refer to the university's Protected Disclosures and Anonymous Reporting Line policy 3364-15-05.

(e) Direct reporting.

Should institutional members feel that the issues or concerns are not being addressed by administration; the institutional member may file a complaint directly to the government or supporting agency. Whistleblower methods may grant the institutional member compensation should the complaint meet the requirements set by the government or agency in question.

Below is a listing of direct reporting examples. This list is not inclusive, and serves as a guideline.

(i) Department of justice (DOJ);

(ii) Prosecuting attorneys;

(iii) Accreditation organizations, such as joint commission

(3) Investigation procedure to be conducted:

(a) Direct an expedient investigation of alleged problem or incident;

(b) If applicable, solicit the support of the office of internal audit, general counsel, and departments specific to the issue and external resources with knowledge of the applicable laws and regulations and required policies, procedures or standards that relate to the specific problem in question;

(c) Interview the complainant and other persons who may have knowledge of the alleged problem or process and a review of the applicable policies, laws and regulations which might be relevant to or provide guidance with respect to the appropriateness or inappropriateness of the activity in questions, to determine whether or not a problem actually exits;

(d) Conduct interviews with person or persons in the departments and institutions who appeared to play a role in the process in which the problem exists. The purpose of the interview will be to determine the facts related to the alleged incident;

(e) Identify and review documents, files and information submitted to the university or other materials to determine the nature of the problem, the scope of the problem, the frequency of the problem, the duration of the problem and the potential financial magnitude of the problem;

(f) Determine if the review results in conclusions or findings that the issue is permitted under applicable laws, regulations or policy or that the incident did not occur as alleged or that it does not otherwise appear to be a problem, if so, the investigation will then be closed;

(g) Determine if the initial investigation concludes that there is improper activity occurring, that practices are occurring which are contrary to applicable law, that potentially fraudulent behavior is taking place, or that additional evidence is necessary, if so, the investigation will then proceed;

(h) Build summary documentation that accurately reflects all investigation findings.

(4) Investigation documentation to be conducted by the internal audit and compliance department

(a) Completion of a report for each reported incident;

(b) Entry of incident information into electronic record-keeping system;

(c) Assignment of an incident number to each reported incident for tracking reasons;

(d) Preparation of a summary report for each reported incident which:

(i) Defines the nature of the problem

(ii) Summarizes the investigation process

(iii) Identifies any person whom the investigator believes to have either acted deliberately or with reckless disregard or intentional indifference toward the university policies, rules and standards

(iv) If possible, estimates the nature and extent of the resulting problems

(e) Retention of incident information, evidence, and history in a retrievable format for future analysis or to the extent the law requires;

(f) Implementation or usage of controls to prevent unauthorized modification, viewing, sharing or destruction of information collected.

(5) Training.

All institutional members, where appropriate, will be trained on appropriate reporting of security incidents.

(E) Enforcement

The failure of any institutional member to perform any obligation required of this policy or applicable local, state and federal laws or regulations will be subject to established University disciplinary actions and/or prosecution by state or federal authorities.

Approved by: Sharon L. Gaber, Ph.D. President May 10, 2016 Date *Review/Revision Completed by:* *Director of Internal Audit and Chief Compliance Officer*	**Policies Superseded by This Policy:** • *Previous 3364-15-03, effective date August 1, 2008* Initial effective date: August 1, 2008 Review/Revision Date: June 1, 2016 Next review date: June 1, 2019