3.1 POLICY ON CONFIDENTIALITY

(a) Purpose and Scope

(1) Purpose. The Maryland Judicial Branch has possession of and access to confidential data and information, in paper and electronic form, that, by law, rule, or policy is not accessible without authorization. An employee within the Judicial Branch may have access to such data and/or information, or other information that is legally privileged. It is essential that employees understand and acknowledge the critical importance of ensuring that the confidentiality of such data and information is maintained at all times, both during and after the course of employment. Section (c) identifies responsibilities and requirements of employees in maintaining the confidentiality of Judicial Branch data and information.

(2) Scope

(A) This policy applies to:
  (i) applicants for employment; and
  (ii) all persons employed by a court, unit, or judicial entity organized within the Judicial Branch
    (I) including regular, temporary, and contractual employees;
    (II) regardless of the source of the employee's compensation (*e.g.*, county, state, federal, grant).

(B) This policy does not apply to:
  (i) the employees of the Register of Wills or the Orphans' Court; and
  (ii) judges, except to the extent that certain judges serve as the administrative head of a judicial entity and, therefore, perform administrative duties consistent with this policy.

(b) Definitions

(1) Administrative Head:

(A) For the Appellate Courts, the Clerk of the Court for all employees under the Clerk's supervision and the Chief Judge of the Appellate Court where the employee works for all other Appellate Court employees;
(B) The Clerk of the Circuit Court for all employees under the Clerk's supervision;
(C) The County Administrative Judge for all employees under the supervision of the Administrative Judge;
(D) For the District Court, the Chief Judge of the District Court, the Chief Clerk, the Administrative Clerk, or the Administrative Commissioner for all employees under his or her supervision;
(E) For the Administrative Office of the Courts (AOC), the State Court Administrator;
(F) For units organized within the Judicial Branch, the head of the unit where the employee works; and,
(G) Any person who, by express written designation, serves as the authorized designee of an administrative head.

(2) Confidential Data and/or Information – Data and/or information, whether in paper or electronic form, that the Judicial Branch is prohibited by Rule, law, or policy from disclosing, including but not limited to:

(A) Case data;
(B) Personnel data;
(C) Financial data;
(D) Trade secrets;
(E) Proprietary information;
(F) Procurement data; and
(G) Administrative records.

(3) Judiciary Human Resources Department (JHRD) – The department within the AOC that is responsible for, but not limited to, the following functions for State-funded employees within the Judicial Branch: human resources policy development, administration, and interpretation; recruitment; employment and orientation services; employee benefits; position classification and salary administration; and employer-employee relations.

(4) Unit - The Attorney Grievance Commission, the Client Protection Fund, the State Board of Law Examiners, the Thurgood Marshall State Law Library, the Commission on Judicial Disabilities, and the Maryland Court of Appeals Standing Committee on Rules of Practice and Procedure.

(c) Employee Responsibilities: Employee responsibilities, with respect to maintaining the confidentiality of the Judicial Branch's data and information, include, but are not limited to:

(1) An employee shall not during, or at any time following Judicial Branch employment, use, permit to be used, misuse, or divulge to individuals who are not authorized to receive any confidential or legally privileged data and/or information obtained during the course of employment.

(2) An employee shall not intentionally access, attempt to access, reproduce, or disclose any confidential or legally privileged data and/or information, whether in paper or electronic form, unless it is necessary for the performance of the employee's duties.

(3) If an employee mishandles, improperly divulges, or improperly acquires confidential information, the employee will immediately inform his or her administrative head.

(4) The Maryland Judiciary shall, at all times, be considered the owner of all research, notes, data, data bases and applications, computations, and estimates or other such information, recordings, videos, work-related emails, and documents, or other work product obtained or created during the performance of the employee's duties, and of any memoranda, reports or other work product resulting therefrom; and an employee will not use or share any of these materials or information during or after employment with the Maryland Judiciary except as necessary to perform his or her duties or as expressly allowed by the Maryland Judiciary.

(5) Upon the termination of employment, an employee will return to the employee's administrative head all work product and confidential documents which the employee created or to which the employee had access during his or her employment, including but not limited to, reports, manuals,

computer programs, and all other materials relating in any way to the business of the Judicial Branch. The employee will not allow any third party to examine or make copies of the employee's work product or confidential documents.

(6) Upon termination of employment, the employee will return, to the employee's administrative head, any electronic device belonging to the Judicial Branch that stores confidential information created or accessed as a result of the employee's relationship with the Judiciary; the employee will not attempt to access that device or disseminate any Judiciary-related data or information stored within it; and the employee will destroy all Judiciary-related information that he or she stored on personal devices during the period of employment.

(7) When in doubt as to whether data and/or information is confidential or legally privileged, an employee shall consult with management before disseminating the data and/or information.

(d) Failure to Comply: A violation of any provision of this policy may result in:

(1) Disciplinary action against the employee, up to and including termination of employment, as determined by the appropriate administrative head;
(2) Injunctive relief;
(3) Damages; and
(4) Criminal liability.

(e) Interpretive Authority: The JHRD, in consultation with other Judicial Branch offices, as appropriate, is responsible for the interpretation of this policy.