WEST VIRGINIA CODE: §29B-1-4

§29B-1-4. Exemptions.

(a) There is a presumption of public accessibility to all public records, subject only to the following categories of information which are specifically exempt from disclosure under this article:

(1) Trade secrets, as used in this section, which may include, but are not limited to, any formula, plan, pattern, process, tool, mechanism, compound, procedure, production data, or compilation of information which is not patented which is known only to certain individuals within a commercial concern who are using it to fabricate, produce, or compound an article or trade or a service or to locate minerals or other substances, having commercial value, and which gives its users an opportunity to obtain business advantage over competitors;

(2) Information of a personal nature such as that kept in a personal, medical, or similar file, if the public disclosure of the information would constitute an unreasonable invasion of privacy, unless the public interest by clear and convincing evidence requires disclosure in this particular instance: *Provided*, That this article does not preclude an individual from inspecting or copying his or her own personal, medical, or similar file;

(3) Test questions, scoring keys, and other examination data used to administer a licensing examination, examination for employment, or academic examination;

(4)(A) Records of law-enforcement agencies that deal with the detection and investigation of crime and the internal records and notations of such law-enforcement agencies which are maintained for internal use in matters relating to law enforcement;

(B) Records identifying motor vehicles used, and the agencies using them, for undercover investigation activities conducted by state law-enforcement agencies or other agencies that are authorized by this code to use undercover or unmarked vehicles;

(5) Information specifically exempted from disclosure by statute;

(6) Records, archives, documents, or manuscripts describing the location of undeveloped historic, prehistoric, archaeological, paleontological, and battlefield sites or constituting gifts to any public body upon which the donor has attached restrictions on usage or the handling of which could irreparably damage the record, archive, document, or manuscript;

(7) Information contained in or related to examination, operating or condition reports prepared by, or on behalf of, or for the use of any agency responsible for the regulation or supervision of financial institutions, except those reports which are by law required to be published in newspapers;

(8) Internal memoranda or letters received or prepared by any public body;

(9) Records assembled, prepared, or maintained to prevent, mitigate, or respond to terrorist acts or the threat of terrorist acts, the public disclosure of which threaten the public safety or the public health;

(10) Those portions of records containing specific or unique vulnerability assessments or specific or unique response plans, data, databases and inventories of goods or materials collected or assembled to respond to terrorist acts; and communication codes or deployment plans of law-enforcement or emergency response personnel;

(11) Specific intelligence information and specific investigative records dealing with terrorist acts or the threat of a terrorist act shared by and between federal and international law-enforcement agencies, state and local law-enforcement, and other agencies within the Department of Homeland Security;

(12) National security records classified under federal executive order and not subject to public disclosure under federal law that are shared by federal agencies and other records related to national security briefings to assist state and local government with domestic preparedness for acts of terrorism;

(13) Computing, telecommunications, and network security records, passwords, security codes, or programs used to respond to or plan against acts of terrorism which may be the subject of a terrorist act;

(14) Security or disaster recovery plans, risk assessments, tests, or the results of those tests;

(15) Architectural or infrastructure designs, maps, or other records that show the location or layout of the facilities where computing, telecommunications, or network infrastructure used to plan against or respond to terrorism are located or planned to be located;

(16) Codes for facility security systems; or codes for secure applications for facilities referred to in subdivision (15) of this subsection;

(17) Specific engineering plans and descriptions of existing public utility plants and equipment;

(18) Customer proprietary network information of other telecommunications carriers, equipment manufacturers and individual customers, consistent with 47 U.S.C. §222;

(19) Records of the Division of Corrections, Regional Jail and Correctional Facility Authority and the Division of Juvenile Services relating to design of corrections, jail and detention facilities owned or operated by the agency, and the policy directives and operational procedures of personnel relating to the safe and secure management of inmates or residents, that if released, could be used by an inmate or resident to escape a facility, or to cause injury to another inmate, resident, or to facility personnel;

(20) Information related to applications under §61-7-4 of this code, including applications,

supporting documents, permits, renewals, or any other information that would identify an applicant for or holder of a concealed weapon permit: *Provided,* That information in the aggregate that does not identify any permit holder other than by county or municipality is not exempted: *Provided, however*, That information or other records exempted under this subdivision may be disclosed to a law-enforcement agency or officer: (i) To determine the validity of a permit, (ii) to assist in a criminal investigation or prosecution, or (iii) for other lawful law-enforcement purposes;

(21) Personal information of law-enforcement officers maintained by the public body in the ordinary course of the employer-employee relationship. As used in this paragraph, "personal information" means a law-enforcement officer's Social Security number, health information, home address, personal address, personal telephone numbers, and personal email addresses and those of his or her spouse, parents, and children as well as the names of the law-enforcement officer's spouse, parents, and children;

(22) Information provided by a person when he or she elects to remain anonymous after winning a draw game prize, pursuant to §29-22-15a of this code; and

(23) Individually identifiable customer information created or maintained by a city or county or other public entity providing utility services in connection with the ownership or operation of a publicly-administered utility enterprise, including, but not limited to, customer names, addresses, and billing and usage records. Nothing contained herein is intended to limit public disclosure by a city or county of billing information:

(A) That the city or county determines will be useful or necessary to assist bond counsel, bond underwriters, underwriters' counsel, rating agencies or investors or potential investors in making informed decisions regarding bonds or other obligations incurred or to be incurred with respect to the publicly-administered utility enterprise;

(B) That is necessary to assist the city, county, state, or public enterprise to maintain the integrity and quality of services it provides; or

(C) That is necessary to assist law enforcement, public safety, fire protection, rescue, emergency management, or judicial officers in the performance of their duties.

(b) As used in subdivisions (9) through (16), inclusive, subsection (a) of this section, the term "terrorist act" means an act that is likely to result in serious bodily injury or damage to property or the environment and is intended to:

(1) Intimidate or coerce the civilian population;

(2) Influence the policy of a branch or level of government by intimidation or coercion;

(3) Affect the conduct of a branch or level of government by intimidation or coercion; or

(4) Retaliate against a branch or level of government for a policy or conduct of the

government.

(c) The provisions of subdivisions (9) through (16), inclusive, subsection (a) of this section do not make subject to the provisions of this chapter any evidence of an immediate threat to public health or safety unrelated to a terrorist act or the threat of a terrorist act which comes to the attention of a public entity in the course of conducting a vulnerability assessment response or similar activity.