WEST VIRGINIA SECRETARY OF STATE
KRIS WARNER
ADMINISTRATIVE LAW DIVISION

eFILED
10/21/2026 7:53:43 AM
Office of West Virginia
Secretary Of State

NOTICE OF RULE MODIFICATION OF A PROPOSED RULE

AGENCY: Office of Technology

RULE TYPE: Legislative TITLE-SERIES: 163-03

RULE NAME: Cyber Reporting

CITE AUTHORITY: § 5A-6C-3 and 5A-6B-3

The above proposed Legislative rules, following review by the Legislative Rule Making Review Committee, is hereby modified as a result of review and comment by the Legislative Rule Making Review Committee. The attached modifications are filed with the Secretary of State.

BY CHOOSING 'YES', I ATTEST THAT THE PREVIOUS STATEMENT IS TRUE AND CORRECT.

Yes

Misty Peal -- By my signature, I certify that I am the person authorized to file legislative rules, in accordance with West Virginia Code §29A-3-11 and §39A-3-2.

TITLE 163
LEGISLATIVE RULE
WEST VIRGINIA OFFICE OF TECHNOLOGY

SERIES 3
CYBER REPORTING

§ 163-3-1. General ~~Provisions~~.

1.1. Scope. -- This legislative rule establishes requirements relating to reporting of cyber incidents. This rule applies to all state agencies within the executive ~~agencies~~ branch, constitutional ~~offices~~ officers, local government entities, ~~and~~ county boards of education, the Judiciary, and the Legislature, as identified by W. Va. Code §5A-6C-2.

1.2. Authority. -- W. Va. Code §5A-6C-3 and §5A-6B-3.

1.3. Filing Date. -- ~~March 27, 2026.~~

1.4. Effective Date. -- ~~April 1, 2026.~~

1.5. Sunset Provision. -- This rule shall terminate and have no further force or effect upon the expiration of August 1, ~~2031~~ 2032.

§163-3-2. Definitions.

2.1. “Cyber attack” means an attack via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure; or destroying the integrity of data or stealing controlled information.

2.2. "Cyber Incident" means any event that threatens the confidentiality, integrity, or availability (CIA) of information assets.

2.3. “Cybersecurity Incident” ~~or “incident”~~ means a violation~~, or imminent threat of a violation, of computer security policies, acceptable use policies, or~~ of standard security practices; an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of the state network or the information the network processes, stores, or transmits; or a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

~~2.3.~~ 2.4. “Cybersecurity Office” means the office within the West Virginia Office of Technology (WVOT), created in W. Va. Code §5A-6B-1.

~~2.4.~~ 2.5. “Cyberspace” means a global domain within the information environment consisting of the interdependent network of information systems infrastructures, including the Internet, telecommunications networks, computer systems, or embedded processors and controllers.

~~2.5.~~ 2.6. “Entity” means the State of West Virginia, including any department, division, agency, bureau, board, commission, office or authority thereof, any political subdivision of the State of West Virginia including, but not limited to, any county, municipality, or school district.

2.7. “Incident” means a cybersecurity incident or cyber incident.

~~2.6~~ 2.8. "Personally Identifiable Information" or "PII", means ~~any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means~~ information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as health, tax, social security, medical, educational, financial, criminal justice, or employment information.

~~2.7. "Protected Health Information" means individually identifiable health information that is transmitted by electronic media, maintained on electronic media, or transmitted and maintained in any other form or medium. Protected health information does not include individually identifiable health information in education records covered by the Family Education Rights and Privacy Act, as amended, 20 U.S.C. 1232g; records described at 20 U.S.C. 1232g(a)(4)(B)(iv); or employment records held by a covered entity in its role as an employer.~~

2.9. "Security Incident" means an occurrence that actually, imminently, or potentially jeopardizes the confidentiality, integrity, or availability of an information system or its data, or constitutes a violation or imminent threat of a security policy.

2.10. "User" means a person performing services for an agency with access to the entity's system, device, account, or network. This includes, but is not limited to, employees, contractors, vendors, automated systems, service accounts, and volunteers.

§163-3-3. Reporting by any entity.

3.1. All entities ~~shall~~ must report ~~qualified cyber~~ security incidents ~~to the Cybersecurity Office via online~~ through the Office of Technology's designated reporting portal, ~~incident.wv.gov~~ within 10 days of discovery of an incident.

3.1.1. Notification to the Cybersecurity Office should be made before any citizen notification of the incident.

~~3.2.~~ 3.1.2. The report ~~of a qualified cyber incident~~ shall not include any ~~personally identifiable information (~~PII~~), protected health information (PHI)~~, passwords, or login information.

§163-3-4. ~~Reporting by~~ Notification requirements for executive branch agencies.

4.1. Any executive branch agency that discovers a ~~cyber~~ security incident, cyber attack, substantial vulnerability, or other electronic threat, ~~shall~~ must immediately, and in no event later than 24 hours after discovering information that supports such a determination, notify the Cybersecurity Office ~~by submitting a report at incident.wv.gov~~ if:

4.1.1. The incident, cyber attack, vulnerability, or threat has an immediate impact on state-owned or state-managed data, devices, systems, or services; or

4.1.2. The incident, cyber attack, vulnerability, or threat can potentially impact state-owned or state-managed data, devices, systems, or services.

4.2. Executive branch agencies must report incidents through the Office of Technology's designated reporting portal.

4.3. The report must not include any PII, passwords, or login information.