WEST VIRGINIA SECRETARY OF STATE
KRIS WARNER
ADMINISTRATIVE LAW DIVISION

eFILED
6/26/2026 1:27:19 PM
Office of West Virginia
Secretary Of State

NOTICE OF PUBLIC COMMENT PERIOD

AGENCY: Office of Technology TITLE-SERIES: 163-03

RULE TYPE: Legislative Amendment to Existing Rule: Yes Repeal of existing rule: No

RULE NAME: CYBER REPORTING

CITE STATUTORY AUTHORITY: W. Va. Code §5A-6C-3 and §5A-6B-3.

COMMENTS LIMITED TO:

Written

DATE OF PUBLIC HEARING:

LOCATION OF PUBLIC HEARING:

DATE WRITTEN COMMENT PERIOD ENDS: 07/25/2026 5:00 PM

COMMENTS MAY BE MAILED OR EMAILED TO:

NAME: Frank J DelGiudice

ADDRESS: Office of Technology

1900 Kanawha Blvd. East; Building 5, 10th Floor

EMAIL: frank.j.delgiudice@wv.gov

PLEASE INDICATE IF THIS FILING INCLUDES:

RELEVANT FEDERAL STATUTES OR REGULATIONS: No

(IF YES, PLEASE UPLOAD IN THE SUPPORTING DOCUMENTS FIELD)

INCORPORATED BY REFERENCE: No

(IF YES, PLEASE UPLOAD IN THE SUPPORTING DOCUMENTS FIELD)

PROVIDE A BRIEF SUMMARY OF THE CONTENT OF THE RULE:

This legislative rule establishes requirements relating to reporting of cyber incidents. It defines terms related to cybersecurity and incident management, outlines who must report cyber incidents, what constitutes an incident, and the method of notification.

SUMMARIZE IN A CLEAR AND CONCISE MANNER CONTENTS OF CHANGES IN THE RULE AND A STATEMENT OF CIRCUMSTANCES REQUIRING THE RULE:

West Virginia Office of Technology is required by statute to manage a central cyber incident reporting portal. The process enables WVOT to maintain security and integrity of state information systems and state data. In response to legislation passed during the 2026 session, the cybersecurity office is updating the associated rule. Proposed changes include removing unnecessary definitions, clarifying who must report, detailing what incidents must be reported, establishing a clear method for reporting, and inserting the website address to access WVOT's online portal.

SUMMARIZE IN A CLEAR AND CONCISE MANNER THE OVERALL ECONOMIC IMPACT OF THE PROPOSED RULE:

A. ECONOMIC IMPACT ON REVENUES OF STATE GOVERNMENT:

The rule should have no direct impact on state revenues.

B. ECONOMIC IMPACT ON SPECIAL REVENUE ACCOUNTS:

The rule should have no direct impact on special revenue accounts.

C. ECONOMIC IMPACT OF THE RULE ON THE STATE OR ITS RESIDENTS:

Mandatory reporting to the West Virginia Office of Technology's online centralized incident management portal provides for quicker evaluation and risk mitigation deployment. This faster response time enables WVOT and agencies to take actions to prevent future data breaches and reduce the impact of events. WVOT can immediately execute any necessary security and data protection steps. The centralized system minimizes data loss, disclosures, and protects state assets. This creates savings by reducing damages, loss, and liabilities.

D. FISCAL NOTE DETAIL:

Effect of Proposal	Fiscal Year		
	2026 Increase/Decrease (use "-")	2027 Increase/Decrease (use "-")	Fiscal Year (Upon Full Implementation)
1. Estimated Total Cost	0	0	0
Personal Services	0	0	0
Current Expenses	0	0	0
Repairs and Alterations	0	0	0
Assets	0	0	0
Other			
2. Estimated Total Revenues			

E. EXPLANATION OF ABOVE ESTIMATES (INCLUDING LONG-RANGE EFFECT):

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, ~~2035~~ 2037.

§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.~~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~~4. “Cybersecurity Office” means the office within the West Virginia Office of Technology (WVOT), created in W. Va. Code §5A-6B-1.

2.~~4~~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~~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~~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. "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~~ incidents to the Cybersecurity Office via the West Virginia Office of Technology's Online Computer Security and Privacy Incident Reporting System ~~online~~ portal at http://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~~1.2. The report ~~of a qualified cyber incident shall~~ must 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~~ an actual or suspected ~~cyber~~ incident, cyber attack, substantial vulnerability, or other electronic threat, ~~shall~~ must immediately 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 use WVOT's Online Computer Security and Privacy Incident Reporting System online portal at-http://incident.wv.gov to report incidents.

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