CYBER SECURITY STANDARD

Standard Identifier:	CSS2019-002
Standard Name:	Advanced Email Protection
Version:	Version 1.0
Cyber Security Framework Alignment:	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders ID.RM-2: Organizational risk tolerance is determined and clearly expressed
Strategic Alignment:	☐ Cyber Risk ☐ Cyber Outreach ☒ Cyber Protection ☐ Cyber Operations
Standard Summary:	Emails sent on behalf of West Virginia State government accounts must 1) be compliant with DMARC (Domain-based Message Authentication, Reporting and Conformance); and 2) have valid and aligned SPF (Sender Policy Framework) and/or DKIM (DomainKeys Identified Mail) records. (See Definitions.)
Standard Details:	Within 180 days, DMARC Conformance for Enterprise Email will be set to “Quarantine” email that fails DMARC requirement. Within 180 days after “Quarantine”, agencies that use a service, secondary site or application to send emails from “@WV.GOV” emails, must pass DMARC by properly authenticating against established DKIM and SPF standards. Emails that fail to meet this standard will be set to “fail” delivery and will not be transported to user mailboxes.
Exceptions Procedure:	WVOT acknowledges that there may be constraints in implementing this Standard. For an agency to be considered for a temporary modification of this Standard, agencies must submit a formal request from Department leadership and Plan of Action and Milestones on correcting the issue.
Questions or Concerns:	Please contact agency or department Interdepartmental Relationship Managers for questions or concerns. Please reference the Request Number in your inquiry.

Issued: August 1, 2019

CYBER SECURITY STANDARD

Issued: August 1, 2019