West Virginia Board of Risk and Insurance Management
Standards of Participation for Insured Entities
October 1, 2004
Revised May 1, 2016

SECTION I – ORGANIZATIONAL SAFETY

1. The entity is expected to develop a safety policy, to have a safety committee and appoint an individual to serve as safety director.

A. The safety policy must be approved by senior management and made available to all employees. All employees must be trained on the policy and the training must be documented.

B. The safety committee in conjunction with the safety director will implement, establish and maintain the entity's loss control program. Duties and responsibilities must be set forth in writing. Safety committee meetings must be held at regular intervals with meeting minutes being maintained.

C. Applicable employees must receive an annual safety performance evaluation as part of their annual review process. Copies of the evaluation must be maintained in writing.

SECTION II – EMPLOYMENT PRACTICES

2. The entity is expected to maintain and follow accepted Personnel Practices.

A. The entity's personnel policies and/or collective bargaining agreements must clearly define the procedures for hiring, promotion, discipline and termination; as well as compliance with EEOC and all applicable federal and state employment laws. Any appeal processes in these policies must be clearly defined.

B. The entity must utilize objective, specific and detailed job descriptions for all positions.

C. The customer must develop and publish an entity-wide policy prohibiting sexual harassment and stating the entity's intolerance of all forms of harassment in the workplace. This policy must provide a clear, open mechanism for reporting allegations of harassment to someone other than the alleged offender.

D. The entity shall conduct criminal background checks, prior to hiring, for all persons being considered for employment in positions that deal with minor children as part of their jobs.

SECTION III – VEHICLE/DRIVER SAFETY

3. The entity is expected to maintain and follow certain guidelines regarding the the operation of entity-owned motor vehicles and equipment

A. Driver selection

(1) The entity must verify that prospective driver employees have a valid driver's license and a copy of the license must be kept on file.

(2) The entity will ensure that the employee is qualified to operate the type of vehicle to which he or she is assigned.

(3) The entity will periodically review the employee's knowledge of safe vehicle operations and safe driving techniques and conduct necessary training in this regard.

B. Driver training

Drivers must be trained on the proper operation and use of entity vehicles and equipment they will operate, and each must demonstrate his or her ability to properly operate such vehicles or equipment. All such training will be documented in writing.

C. Vehicle maintenance and repair

(1) All entity vehicles must be maintained in compliance with all state and federal laws.

(2) Regular preventative maintenance must be performed on all vehicles, with appropriate records kept on each vehicle. All repairs and maintenance must be in accordance with the manufacturer's recommendations.

D. Accident investigation

(1) The entity must thoroughly investigate all accidents to determine the root cause(s) for the accidents. Once identified, the entity must take such measures as may be necessary to prevent similar accidents from occurring in the future. This may require such actions as driver re-training, policy revision and employee discipline.

(2) All employees must be informed of and trained on the proper accident investigation procedure.

E. Driver recognition

The entity will maintain a program to recognize safe drivers and accident free driving.

SECTION IV – FACILITY SAFETY

4. The entity is expected to properly inspect and maintain its facilities.

A. The entity must conduct and document self-inspections of its buildings and facilities at least semi-annually. Appropriate action must be taken to correct the deficiencies noted during these inspections.

B. Deficiencies and repairs must be prioritized and corrected according to their importance based on life safety and cost.

C. Fire and security alarms as well as fire detection systems must be installed as may be required by code.

SECTION V – COOPERATION WITH BRIM LOSS CONTROL EFFORTS

5. The entity is expected to participate in, and cooperate with the loss control efforts undertaken by the Board of Risk and Insurance Management (BRIM).

A. The entity must actively participate in loss prevention/safety surveys and ensuing discussions with regard to strategies necessary for controlling losses.

B. The entity must provide a written response, within forty-five days, for all BRIM loss control recommendations, including those prepared by any loss control vendor hired by BRIM.

C. After providing the above required written response, the entity must, within ninety days, implement substantially all of the BRIM proposed loss prevention and safety recommendations; or submit an alternative plan, which must be approved by BRIM, for addressing the recommendations.

SECTION VI – CYBER/INFORMATION SECURITY AND PRIVACY

6. A. The entity is expected to ensure that all employees, board members, volunteers and other member of its workforce sign an appropriate Confidentiality Agreement.

(1) The Confidentiality Agreement must be signed upon hire and as otherwise required by law, policy, or procedure, whichever is more restrictive.

(2) The entity shall provide access to all applicable confidentiality policies and procedures to each member of its workforce.

(3) The Confidentiality Agreement must state that it shall survive the termination of employment or other workforce arrangement, including transfer to other entities or termination of the contractual relationship.

B. The entity is expected to maintain and follow its privacy policies.[1]

(1) The entity has privacy policies which are documented in writing that includes the following:

- Accountability
- Consent
- Individual Rights
- Minimum Necessary and Limited Use
- Notice
- Security Safeguards
- Incident Response Procedure

(2) The privacy policies are made readily available to internal personnel and third parties, including vendors and the public.

(3) The Incident Response Procedure includes an appropriate response to breaches or incidents that threaten the confidentiality, integrity, and availability of information assets, information systems, and the networks that deliver them.

C. The entity is expected to provide privacy and security awareness training to its employees on a periodic basis.

(1) The privacy awareness training includes information about the entity's privacy policies and related matters. It is required every two years for all employees, board members, volunteers, and other members of the workforce. Documentation of training must be maintained by the entity.

(2) The security awareness training is required annually for all employees, board members, volunteers, and other members of the workforce and should include information about the entity's security policies and related matters. Documentation of the training must be maintained by the entity.

(3) New employees, board members, volunteers, and other members of the workforce are required to complete these courses within the first month following employment in order to retain their access privileges. Documentation of the training must be maintained by the entity.

D. The entity is expected to retain personal information for no longer than necessary to fulfill the stated purposes unless a law or regulation requires otherwise. Additionally, when personal information is no longer retained, it is anonymized, disposed of, or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access.

(1) The entity shall document its record retention policies and disposal procedures.

[1] Definitions of these terms and example policies and procedures may be found at www.privacy.wv.gov and www.brim.wv.gov.

(2) The entity shall ensure that personal information is not kept beyond the specified retention time, unless a justified business or legal reason for doing so exists.

(3) The entity shall document disposal of personal information. Paper, film, or other hard copy media must be shredded or destroyed such that the personal information cannot be read or otherwise reconstructed. Electronic media must be cleaned, purged, or destroyed such that personal information cannot be retrieved.

E. The entity has implemented a policy to categorize information and information systems that takes into account the potential risk.

(1) Information systems are protected by the selection of management, operational, and technical security controls that are directly proportionate to the risk to each system.

(2) The entity documents cyber risk, and develops plans to avoid, accept, mitigate or transfer risk based on the criticality of information systems.

(3) The entity concentrates security resources on the most critical data assets as a best practice, with a layered approach that fits the specific business needs of the entity.

F. The entity requires data-at-rest protection (encryption) on all entity-owned laptop computers, tablets and smartphones.

(1) The entity ensures that end-user devices are secured by encryption and maintained properly to reduce the risk of compromise or misuse. Such devices should be annually audited for encryption protection.

(2) The entity policies and processes incorporate appropriate usage of the storage encryption solution and provide the foundation for the planning and implementation of storage encryption.

(3) Employees, board members, volunteers, and other members of its workforce are trained on proper use of encrypted devices.

G. The entity shall have Information Systems that require strong authentication and shall regularly require audit of account access and permissions.

(1) The entity develops, disseminates, and reviews a formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

(2) The entity tracks and monitors Information System accounts for (i) valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the entity or associated business functions.

(3) The entity manages Information System accounts, by establishing, activating, modifying, disabling, and removing accounts; where applicable, and in accordance with policy.

(4) Authentication of user identities is accomplished through the use of strong passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof.

H. The entity completes vulnerability scanning of information systems, at a minimum of quarterly, and ensures findings are remediated in accordance with a risk management methodology.

(1) Vulnerability scanning is completed, at least quarterly, to prevent attacks and reduce the potential impact of successful ones. Monthly vulnerability scanning is an industry best practice.

(2) The entity accurately plans for vulnerability assessments by providing guidance on which systems to assess, addressing logistical considerations, developing an assessment plan, and ensuring that legal and policy considerations are addressed.

(3) The entity conducts root-cause analysis upon completion of an assessment to enable the translation of findings into actionable mitigation plans.

(4) Assessment findings are remediated based on risk to information systems.

I. The entity maintains and follows a backup policy and procedures for the protection of critical information systems and critical data.

(1) The entity has a detailed information system information plan, containing guidance and procedures for restoring a system, unique to the system's security impact level and recovery requirements.

(2) The entity requires that all critical information systems are backed up.

(3) The entity ensures coordination with internal and external points of contact and vendors associated with critical information systems to execute backup policy and procedures.

SECTION VII – ADDITIONAL STANDARDS (AS APPLICABLE)

7. The entity is expected to perform appropriate sewer maintenance (*Public Service Districts and water departments)*.

A. The entity must establish and maintain a scheduled and documented sewer maintenance and inspection program. Appropriate action must be taken to correct the deficiencies noted during inspections.

B. To the extent possible and/or practicable, storm water runoff and sewer water shall be kept separate.

8. Entities involved in law enforcement are expected to maintain certain policies and procedures with regard to police operations.

A. The entity must formally designate a training officer.

B. The entity must have appropriate written policies and procedures that cover at least the Following areas:

(1) Resolving confrontations using non-physical means
(2) Use of force [lethal and non-lethal]
(3) Vehicle pursuit
(4) Search and seizure and the use of the *Miranda* warning
(5) Arrest and custody of suspects and prisoners
(6) Domestic violence
(7) Diversity and tolerance
(8) Prevention of sexual abuse of persons in custody
(9) Racial and other types of profiling
(10) Properly reporting unlawful or improper actions by other officers

C. The entity must conduct weapons training for all officers at least once annually.