VMI Data Breach Notification Policy

Purpose

The purpose of this policy is to specify the notification requirements for the Virginia Military Institute (VMI) by identifying the triggering factors and necessary responses to unauthorized release of unencrypted sensitive information. This policy shall be observed by VMI and any third party agency or organization to which VMI has entered an Interoperability Security Agreement Memorandum of Understanding (ISA).

Requirements

1) Identification of all systems, processes, and logical and physical data storage locations (whether held by VMI or a third party) that contain Personally Identifiable Information (PII) meaning an individual's name and any of the following:
   a) Social Security Number
   b) Driver's license or Identification card number
   c) Financial account number, credit or debit card number
   d) Other personal identifying information, such as insurance data or date of birth.
2) VMI systems, processes, and logical and physical data storage locations containing PII as outlined above are specified in the "Information Technology Risk Management and Assessment" document.
3) Any third party contractor, subcontractor, organization, or agency with which VMI has entered an ISA must provide immediate notification to VMI of suspected breaches; and allow VMI both to participate in the investigation of the incidents and exercise control over decisions regarding external reporting.
4) The VMI or any third party contractor, subcontractor, organization, or agency with which VMI has entered an ISA must provide appropriate notice to affected individuals upon the unauthorized release of unencrypted PII by any mechanism, including, but not limited to:
   a) Theft or loss of digital media including laptops, desktops, tablets, CD's, DVD's, tapes, USB drives, SD cards, etc.;
   b) Theft or loss of physical hardcopy; or
   c) Security compromise of any system. The agency shall provide this notice without undue delay as soon as verification of the unauthorized release is confirmed, except as delineated below in the "Large scale breaches" section.
5) Appropriate notification to individuals consists of:
   a) A general description of what occurred and when;
   b) The type of PII that was involved;
   c) What actions have been taken to protect the individual's personal information from further unauthorized disclosure;
   d) What, if anything, the agency will do to assist affected individuals, including contact information for more information and assistance; and
   e) What actions the agency recommends that the individual take.
6) Notification shall be provided by one or more of the following methodologies, listed in order of preference:
   a) Standard mailing to any affected individuals whose mailing addresses are available.
   b) Electronic mail to any affected individuals whose email address has been provided to the agency as a contact mechanism.
   c) In the case of large scale breaches or data breaches where neither form of communication listed above is available or feasible, public communications channels, including:
      i) Conspicuous notification on the agency website; and
      ii) Notification by statewide public media, including newspaper, radio, and television).
7) Notification shall not be immediately provided following verification of unauthorized data disclosure only if requested by:
   a) Law Enforcement entities where it would interfere with an ongoing investigation; or
   b) Chief Information Security Officer of the Commonwealth of Virginia or designee where it would interfere with a determination of the scope of the data breach or investigation of root cause.