

## Virginia Department of Education

### Information Technology Security Policy Statement

**Purpose:** The purpose of the Information Technology (IT) Security Program is to protect the Virginia Department of Education's (VDOE) information technology assets and the data by defining the information technology security program for the Department.

**Background:** The VDOE relies heavily on the application of information technology for effective delivery of services to Virginia citizens, school divisions, and other stakeholders.

As such, the security and protection of information technology and data is critical to the performance of our mission. Continual and rapid advances in information technology serve to increase our dependence on it.

It is recognized that data, software, hardware, and telecommunications are vital assets that must be protected.

The Information Security Program is built to support the mission of the VDOE and to maintain public trust. This program provides an approach that must be replicated across all VDOE information technology assets to give the highest levels of information and data assurance and allow best industry practices to prevail.

**Guiding Principles:** The following principles guide the Information Security Program.

- a. VDOE data is critical to the operation and mission of the Department and access to that data is restricted to persons authorized to use it for official business.
- b. Information security is the cornerstone of maintaining public trust; it must be managed to address both business and technology requirements of the Department, be risk-based, cost effective, and align with Commonwealth of Virginia (COV) priorities, industry best practices and government laws, regulations, and requirements.
- c. Information security is directed by management as policy, but implemented by the employees and contractors in each business unit. Ultimately it is the responsibility of all who use VDOE IT systems and data to protect these vital assets.

**Application:** The program is applicable to all VDOE employees and contractors that manage, develop, purchase, and use the information technology resources of the Department of Education and/or those of the Virginia Information Technologies Agency/Northrop Grumman Partnership (VITA/NG).

**Policy:** This policy adopts the policies and standards set forth in the Commonwealth's Information Technology Resource Management (ITRM) Information Security Policy and Information Security Standard as the guiding precept for the VDOE program which meets or exceeds them.

The VDOE information security program consists of the following areas:

- Risk Management and IT Contingency Planning

- Information Systems Security and Access Control
- Data Protection
- Threat Management
- IT Asset Management

This policy is the framework that the VDOE uses to establish and maintain a prudent security profile that supports the Department and the Commonwealth. Additionally, all data must be handled in accordance with applicable laws and regulations.

The function of this policy is to protect VDOE IT resources from credible threats whether internal or external; deliberate or accidental. Employees must keep in mind that while they may need access to sensitive or confidential data to perform their function, reasonable measures must be in place to protect it.

It is the function of this IT security program to employ all reasonable, prudent, and cost effective IT security measures to:

- a. Protect COV/VDOE information against unauthorized access or use;
- b. Maintain the integrity of COV/VDOE information;
- c. Ensure that information stored on all VDOE systems is available when needed;
- d. Comply with federal, state and other legislative, regulatory and industry requirements; and

Review this policy to ensure it remains valid in the face of changing threats, business needs, and technologies.