State of Illinois
Department of Innovation & Technology
PCI Data Security Policy

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) establishes this Policy to encourage and enhance the security of cardholder data and facilitate the broad adoption of consistent data security measures. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to ensure that State of Illinois agencies, boards, and commissions securely store, process, or transmit cardholder data in compliance with established Payment Card Industry Data Security Standards (PCI DSS).

3. SCOPE

This Policy applies to Users of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT in collaboration with Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" shall include both DoIT and Client Agencies.

4.1 Build and Maintain a Secure Network and Systems

- 4.1.1 Agency shall install and maintain a firewall configuration to protect cardholder data.
- 4.1.2 Agency shall change all vendor-supplied defaults for system passwords and other security parameters.
- 4.1.3 Agency shall protect stored cardholder data from unauthorized access.
- 4.1.4 Agency shall encrypt transmission of cardholder data across open, public networks.

4.2 Maintain a Vulnerability Management System

- 4.2.1 Agency shall protect all systems against malware and shall regularly update anti-virus software or programs.
- 4.2.2 Agency shall develop and maintain systems and applications that are secure from unauthorized access.

4.3 Implement Strong Access Control Measures

- 4.3.1 Agency shall restrict access to cardholder data on a business need-to-know basis.
- 4.3.2 Agency shall identify and authenticate access to system components.
- 4.3.3 Agency shall restrict physical access to cardholder data.

4.4 Regularly Monitor and Test Networks

4.4.1 Agency shall track and monitor all access to network resources and cardholder data.

4.4.2 Agency shall regularly test security systems and processes.

4.5 Maintain an Information Security Policy

4.5.1 Agency shall maintain policies that clearly define information security responsibilities for all personnel.

5. POLICY COMPLIANCE

Compliance with this Policy is accomplished through established procedures and designation of responsibility to specific personnel/job titles. To the extent necessary, each Client Agency shall establish policy, standards, and procedures in accordance with this Policy. Exceptions to this Policy are approved through DoIT where justified in maintaining acceptable levels of assurance.

All authorized Users are responsible for Policy adherence and understanding. Failure to comply with this Policy could result in discipline, up to and including discharge.

6. REVISION HISTORY

Original Effective Date	
Last Review Date	
Revised Date	

7. APPROVALS AND MANAGEMENT COMMITMENT

Effective upon latest signature below.

_____ Date: _____

DoIT Acting Secretary, Kirk Lonbom

_____ Date: _____

Chief Information Security Officer, Chris Hill

_____ Date: _____

DoIT General Counsel, Michael Delcomyn

4.4 Regularly Monitor and Test Networks

4.4.1 Agency shall track and monitor all access to network resources and cardholder data.

4.4.2 Agency shall regularly test security systems and processes.

4.5 Maintain an Information Security Policy

4.5.1 Agency shall maintain policies that clearly define information security responsibilities for all personnel.

5. POLICY COMPLIANCE

Compliance with this Policy is accomplished through established procedures and designation of responsibility to specific personnel/job titles. To the extent necessary, each Client Agency shall establish policy, standards, and procedures in accordance with this Policy. Exceptions to this Policy are approved through DoIT where justified in maintaining acceptable levels of assurance.

All authorized Users are responsible for Policy adherence and understanding. Failure to comply with this Policy could result in discipline, up to and including discharge.

6. REVISION HISTORY

Original Effective Date	
Last Review Date	
Revised Date	

7. APPROVALS AND MANAGEMENT COMMITMENT

Effective upon latest signature below.

DoIT Acting Secretary, Kirk Lonbom — Date: 10/8/18

Chief Information Security Officer, Chris Hill — Date: 9/22/18

DoIT General Counsel, Michael Delcomyn — Date: 10/15/18