2016 GENERAL ELECTION

LESSONS LEARNED

Voting Machine Security

Cybersecurity

Physical Security

Who and How?

Statewide Seal Use Protocols

- Seal use protocol training class is required
- Criminal background check is required
- State purchases voting machine seals
- Vendor must be ISO 9001 certified
- Seal inspections before and after any election is required
- Voting machine delivery tracking is required

Statewide Pre-election Testing Protocols

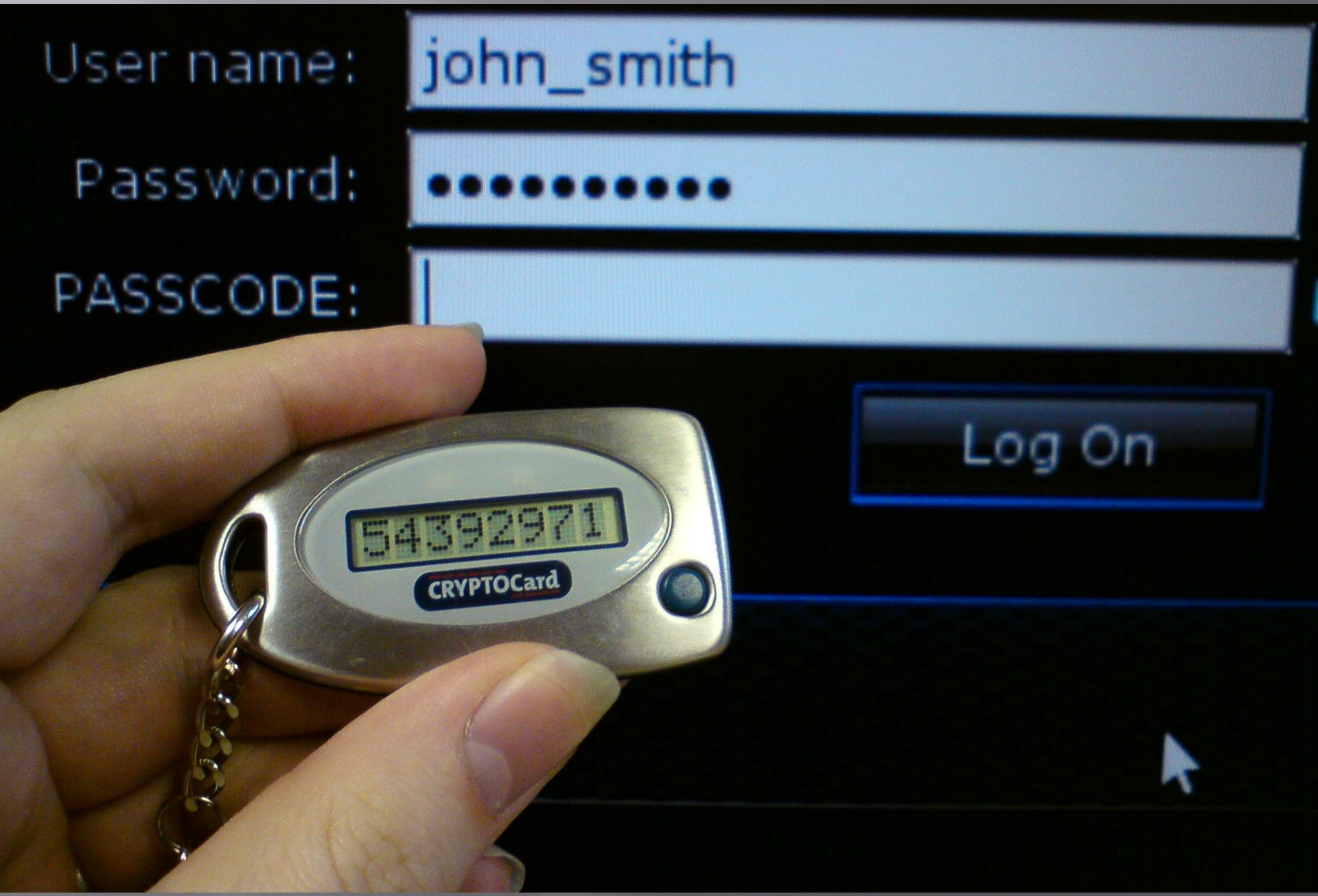
- Maintenance Diagnostics or Preventative Maintenance
- Ballot verification
- Test voting (Ascending or Descending Pattern)

Access to Voting Machines

- Election Officials
  - Password Strength
    - Length, Special Characters, Expiration
  - Multifactor or Two Factor Authentication
    - Something you have and something you know


SMART CARD
07/17


RSA
SecurID®
159 759.
Secured by RSA


User name:
john_smith
Password:
PASSCODE:
Log On
54392971
CRYPTOCard

Access to Voting Machines

- Manufacturers
  - Company Ownership
  - Company Policies and Procedures

NJ Office of Information Technology
Chris Christie, Governor
E. Steven Emanuel, Chief Technology Officer

P.O. Box 212 www.nj.gov/it/ps/
300 Riverview Plaza
Trenton, NJ 08625-0212

STATE OF NEW JERSEY IT CIRCULAR

Title: 169-00-01 – Business Entity, IT Services and/or Extranet

NO:	SUPERSEDES:
09-11-P1-NJOIT	N/A
LAST REVIEWED: January 22, 2015	**DATE PUBLISHED:** August 7, 2009
VERSION: 2.0	**EFFECTIVE DATE:** Date of Signature
FOR INFORMATION CONTACT: Office of Policy and Planning	

ATTN: Directors of Administration and Agency IT Managers

I. PURPOSE

The purpose of these procedures is to establish access rules, security expectations and responsibilities for the Sponsoring Agencies and Business Entities when Information Technology (IT) services are planned, or are made available to agencies, and/or when establishing an operating an extranet connection(s) to the State of New Jersey Next Generation Services Network (NGSN) for conducting electronic business with the State of New Jersey.

II. AUTHORITY

This policy is established under the authority of the State of New Jersey. N.J.S.A. 52:18a-230 b. This policy defines New Jersey Office of Information Technology's (NJOIT) role with regard to technology within the Executive Branch community of State Government.

The New Jersey Office of Information Technology (NJOIT) reserves the right to change or amend this circular.

III. SCOPE

These procedures apply to all personnel including, business entities, employees, temporary workers, volunteers, contractors and those employed by contracting entities, and others who are authorized to access enterprise information resources and/or systems regardless of what technology is used for the connection.

IV. DEFINITIONS

Please refer to the statewide policy glossary at http://www.state.nj.us/it/ps/glossary/index.html.

V. PROCEDURES

A. All Sponsoring Agencies and their Business Entities utilizing an IT and/or Extranet services shall adhere to the following:

1. Sponsoring Agencies that require IT services and/or extranet connectivity to a Business Entity must complete a System Architecture Review. This process is initiated by completing a BCR (Business Case Review) form.
2. Sponsoring Agencies that have completed the business case review and have obtained preliminary approval for IT services and/or extranet connectivity, must file a Business Entity Application form (Appendix A) through the Statewide Office of Information Security.
3. Before any extranet connections are established, the Sponsoring Agency and the Business Entity must execute the Extranet Agreement (Appendix B).
4. The Sponsoring Agency together with the Business Entity and OIT where applicable, must complete the Business Entity Extranet Operational Form (Appendix C).
5. The Sponsoring Agency must maintain all documentation associated with extranet activity. They must review the details of the documentation on a regular basis to ensure the accuracy of the content. They must also notify all parties if any contact information changes.

B. The Business Entity must complete the Security Controls Assessment Checklist (Appendix D). The checklist must be reviewed and approved by the Statewide Office of Information Security prior to the system or application going into production.

1. Any agency that wishes to connect to a pre-existing IT service and/or extranet connection must execute an Extranet Agreement (Appendix B) with the Sponsoring Agency and OIT.
2. When access is no longer required, the Sponsoring Agency must notify OIT's SOIS and WAN groups within 30 days. Staff at these groups will then terminate connectivity.

C. Establishing Agreement

Sponsoring agencies that require connectivity to or from a Business Entity must complete a Business Case Review (BCR) form that can be obtained by sending an email request to sar@oit.nj.gov. The agencies must also participate in the SAR to review the anticipated project, prior to submission of a Business Entity IT Service and/or Extranet Application (Appendix A).

P.O. Box 212 www.nj.gov/it/ps/
300 Riverview Plaza
Trenton, NJ 08625-0212

STATE OF NEW JERSEY
Security Controls Assessment Checklist

Agency/Business (Extranet) Entity

Response

Agency

Agency Name:

Application Name:

Point of Contact:

Telephone Number:

Date:

Business (Extranet) Entity

Name:

Point of Contact:

Telephone Number:

Email Address:

Security Point of Contact:

Telephone Number:

Email Address:

No.	Doc.	Security Control Item	Security Description/Requirements	Response/Acknowledgement
1	T&C	Security Plan	The Contractor must provide a security plan for the proposed solution. The document shall describe the administrative, physical, technical and systems controls to be used by the system and/or services. The Contractor's security plan must, at a minimum, provide security measures for the following areas: ▪ Facilities Physical Security & Environmental Protection ▪ System Security ▪ System Data Security ▪ Network Security ▪ Administrative and Personnel Security The security plan shall provide for review of the Contractor's operations and control system for the proposed solution. The Contractor shall have the capability to detect and report attempted unauthorized entries into the facility and system. All security requirements for the Contractor apply to development, testing, production and backup systems.	
2	T&C		Regulations and security requirements – How the Contractor will address security requirements such as PCI, HIPAA, FISMA and etc.	
3	T&C		System, Administrative and Personnel Security – The security responsibilities and supervision required for information owned and/or operated by the Contractor. Security responsibilities include responsibilities for administration of the infrastructure, implementing or maintaining security and the protection of the confidentiality, integrity, and availability of information systems or processes.	
4	T&C		Workforce Security – The control process for hiring and terminating of Contractor's employees, and method used for granting and denying access to the Contractor's network, systems and applications. Identify and define audit controls when employment of the employee terminates. Identify rules of behavior.	
5	T&C		Role-based security access – The products and methods provide role-based security, access enforcement and least privilege.	

6	T&C		Account Management – The products and methods identify and control the account types to meet defined regulation and security requirements.	
7	T&C	→	Password Management – The appropriate password management controls to meet defined regulation or security requirements.	
8	T&C		Logging/Auditing controls – The Contractor's audit control methods and requirements. The controls must address all user access and user identification linked to any changes to the system and data, and provide an audit process that will make all audit data accessible to state and federal audit staff. The audit trail of all transactions should track date, time, user, and end-user device that initiated the transaction. The audit data must be protected, non-repudiated and restricted to authorized staff. Retention of the audit records will be retained online for at least 90 days and further preserved offline for the period required by the contract or State and Federal laws and regulations.	
9	T&C		Incident Management – The methods for detecting, reporting and responding to an incident, vulnerabilities and threats. The methods are tested and exercised.	
10	T&C	→	Vulnerability/Security Assessment – The products and methods used for scanning for vulnerabilities and remediation of the vulnerabilities. Identify and define methods used for initiating and completing security assessments. All systems and applications shall be subject to vulnerability assessment scans by an independent and accredited third party on an annual basis.	
11	T&C		Application Security – Where the Contractor is providing application hosting or development services, the Contractor at a minimum shall run application vulnerability assessment scans during development and system testing. Vulnerabilities shall be remediated prior to production release.	
12	T&C		Application Partitioning – Where the Contractor is providing application hosting or development services, the Contractor will have a separate and unique (single tenant) partition.	

13	T&C		Anti-virus/malware controls – The products and methods for anti-virus and malware controls meet industry standards. It shall include policy statements that require periodic anti-viral software checks of the system to preclude infections and set forth its commitment to periodically upgrade its capability to maintain maximum effectiveness against new strains of software viruses.	
14	T&C	→	Network Security – Where the Contractor has access to State confidential data, and that data will traverse the Contractor's network, the Contractor shall maintain the Contractor's network security to include, but not be limited to: network firewall provisioning, intrusion detection and prevention, denial of service protection, annual independent and accredited third-party penetration testing. The Contractor shall maintain a hardware inventory including name and network address. The Contractor shall maintain network security that conforms to current standards set forth and maintained by the National Institute of Standards and Technology (NIST), including those at: http://web.nvd.nist.gov/view/ncp/repository	
15	T&C		Database – The products and methods for safeguarding the database(s).	
16	T&C		Data Integrity – The products and methods on the integrity of all stored data and the electronic images, and the security of all files from unauthorized access. The Contractor must be able to provide reports on an as-needed basis on the access or change for any file within the system.	
17	T&C		Server and infrastructure – The products and methods for "hardening" of the hardware's operating systems and software.	
18	T&C		Wireless, Remote and Mobile Access – Where the Contractor has access to State confidential data, and that data traverses the Contractor's network, the Contractor shall have security controls for provisioning accounts, authorization, account/credential verification, audit/logging, VPN, and TCP/UDP ports restrictions.	
19	T&C		Transmission – The products and methods on how its system addresses security measures regarding communication transmission, access and message validation.	
20	T&C		Continuous Monitoring – Where the Contractor has access to State confidential data, and that data will traverse the Contractor's network, the	

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014