State Board of Elections

Credentialing Procedures

Maryland State Board of Elections

March 14, 2010

Version 2

Version History

Revision	Description	Name, Date
1	Revision of contractors' document to become SBE document	Janey Hegarty, Thomas Queen, Michael Kortum on 12.05.2007
2	Revision of contractor's document to become SBE document	Michael Kortum, Janey Hegarty on 03.14.2010

___________________________________ ________________________

Project Manager, SBE Date

Terminology

Term	Definition
MDSBE, SBE	Maryland State Board of Elections
Local Board of Election (LBE)	The County Election Directors and staff who oversee the conduct of all elections held in the county
Credential	The process of providing a state issued photo identification for SBE contractors that acknowledges the recipient has the authority to provide services to or on behalf of the SBE

References

Document	Author	Status	Version
State of Maryland Policy for Conducting Criminal Background Investigations	COMAR		
State of Maryland Criminal History Record Check Procedures	T. Augustine		
Information Technology Security Policy and Standards	DOIT, Secretary, Department of Information Technology		Version 2.2 Oct. 2009

Table of Contents

1 INTRODUCTION

This document defines the Maryland State Board of Elections (SBE) office credentialing process used primarily for contractors supporting the Maryland election process. SBE is required under the Information Technology Security Policy and Standards issued by the Department of Budget and Management Office of Information Technology to ensure sufficient security clearance for all election officials, employees, volunteers and contract personnel who use systems that are deemed sensitive.

2 CREDENTIALING OVERVIEW

SBE maintains that all election volunteers, employees of the SBE and LBEs and contractors working for or in support of the Election offices are required to display a State identification badge. LBEs usually obtain employee identification badges directly through county or State facilities. SBE is required to routinely report on all contractors working in support of the election process therefore SBE will issue all badges to contractors supporting the election. In order to obtain an SBE issued identification badge, the individual must complete the pre-credentialing requirements. This SBE issued badge must be accompanied by a valid state or Federal issued photo identification (example, driver's license or military identification) while performing work at or on behalf of the SBE. Credentialing will be authorized by the State Administrator, Deputy State Administrator, Chief Information Officer, Voting Systems Director, and/or their designees.

This document contains information and guidelines primarily for the use of SBE to implement the Credentialing process. This document will outline the following:

Subject	Applicable Viewer
Process of requesting credentialing	SBE
Reporting protocol (requirements)	

3 ASSUMPTIONS

- These procedures cover badges issued by the credentialing resource, which shall be known as the SBE IT support. Responsibility for proper use management and disposal of the official SBE contractor credentialing documents and badges is a shared responsibility with the SBE management, contractor project officer and the contracted individual.
- Contractors have already submitted to any of the following applicable pre-credentialing requirements of the SBE Chief Information Officer (CIO) or the Chief Information Systems Security Officer (CISSO). Requirements could include but are not limited to:
    - Criminal History Background Investigation (CHBI)
    - Rules of Security Behavior for Board of Elections' Officials and Employees
- Contractors have already submitted to the pre-credentialing requirements of their hiring agency; (example, employment verification and drug testing)

4 REQUEST FOR CREDITIALING SUPPORT

Whether credentialing is requested by an SBE or a vendor resource, the basic process remains the same. The requesting LBE or vendor resource should make the initial request for credentialing by telephone or email to the contract manager, the SBE CIO or CISSO, or their designee five (5) working days but not less than 48 hours prior to the anticipated credentialing date to receive approval.

5 SCHEDULE CREDENTIALING

Once credentialing support is approved, the IT Support or his/her designee will notify the individuals to be credentialed. The resource(s) will contact the person requesting support using the Request for Credentialing Support Form to request services.

6 STEPS USED TO CREATE A BADGE

6.1 Completing the Badge Acceptance Form for Contractors

Before the credentialing resource will create photo identification for a contractor:

1. Each contractor shall read, sign and date the Badge Acceptance Form for Contractors.
2. The credentialing resource shall validate the contractor's identity by checking their valid a state issued photo identification (for example, a driver's license or military identification) against the printed name and signature on the Badge Acceptance Form for Contractors.

►**NOTE:** When necessary, the contractor will also complete the Rules of Security Behavior for Election Officials' and Employees. This usually occurs when the contractor's photo identification is created for short term usage (for example, Election Day Support Staff, Logic & Accuracy resources, Post-Election Maintenance resources).

3. When credentialing is complete, the resource performing the credentialing will return all completed Badge Acceptance Form(s) for Contract Employees to the IT Support for archiving.

6.1.1 Short Term Badges

Badges issued to contractors perform services at or on the behalf of the SBE should be returned at the end of the project to the vendor or supervisor for return to the SBE IT Support.

6.2.2 Long Term Badges

Badges issued to perform services at or on the behalf of the SBE for an extended period should be returned by the supervising vendor to the SBE IT Support.

6.2.3 Returned Badges

Badges that have expired will be reported to the SBE CIO, etc., within 5 business days after receipt by the SBE IT Support. Badges that are no longer needed, due to project termination or other event, will be reported in a consolidated report as a part of the Credentialing Activity Summary. For example, badges issued to temporary technicians supporting precincts in a primary election would be summarized as a part of the post-election Credentialing Activity Summary.

APPENDIX A – POLICY FOR BACKGROUND CHECKS

Purpose

The purpose of this policy is to provide a standard for the use and application of Criminal History Background Investigations (CHBI) by the State Board of Elections (SBE) and local boards of elections (LBEs).

Legal Authority

Pursuant to §§ 3-401 through 3-413 and 3-701 through 3-705 of the State Finance and Procurement Article, the Department of Budget and Management Office of Information Technology is required to develop an *Information Technology Security Policy and Standards (*ITSPS*)*. Specifically, section 8.5 of the ITSPS states:

> Security clearances are required for personnel as determined by the system sensitivity and data classification designation. Agencies will ensure that an appropriate background investigation (e.g., CJIS, State Police) has been completed on personnel as necessary. Agencies will maintain personnel clearance information on file.

In other words, the ITSPS requires agencies to ensure sufficient security clearance for employees who use systems that are deemed by the agency as sensitive. That designation has been made for the voting system and certain aspects of the MDVOTERS system.

Background

The *Rules of Security Behavior for Board of Elections' Officials and Employees* requires election officials and employees to submit to all necessary background checks and receive authorization before having access to sensitive, confidential, or trademark specific information, materials, or equipment. These background checks are necessary to ensure that SBE and LBEs are taking necessary and reasonable steps to protect the confidential voter registration and candidate records and to ensure the security and integrity of the voting system.

Applicability

SBE and LBEs are required to conduct a CHBI of any election official or employee who is initially hired to positions that meet any of the below stipulations as well as an official or employee whose new duties meet any of the below stipulations. These stipulations include:

- Employees who may have any access to and or may manipulate information of those voters or candidates who have been classified as confidential.
- Employees who will be authorized to maintain MDVOTERS servers.
- Employees who will be authorized access to GEMS servers.
- Employees who may be responsible for moving/transporting, storing, securing or working on voting systems and components. This includes:
  - Employees who work in the warehouse with the voting equipment;
  - Employees who conduct L&A testing;
  - Employees who transport voting equipment to or from the polls; and
  - Employees who conduct post election voting equipment maintenance.

Policy

The SBE Chief Information Officer (CIO) or the Chief Information Systems Security Officer (CISSO) shall request a CHBI for all full-time, part-time, permanent and contract employees of the State or Local Boards of Election who have any access to the electronic voting systems or to information designated as confidential in the electronic voter registration systems. At the direction of the CIO or CISSO, a CHBI may be conducted on election judges. The CIO or CISSO shall request the CHBI once for such employees prior to the first election of the year or upon initial employment.

If the CHBI indicates that the employee or contract employee has been found guilty of a crime that is included on the list of infamous as revised annually by the Office of the Attorney General, the CIO or CISSO shall prohibit such employee or contract employee from preparing, programming, operating, using or having any access to all components of the electronic voting systems or confidential voter registration information.

APPENDIX B – CRIMINAL HISTORY RECORD CHECK PROCEDURES

Supplies Needed — Fingerprint Card and Instructions

❑ 1 Maryland Application for Criminal History Record Check Fingerprint Card (CJIS-012, purple)

❑ Instructions for completing the State of Maryland Application for Criminal History Record Check

❑ **Complete ONLY the portion from Name through Position Applied For and the Disclosure on the reverse side**

Scheduling and Payment for Fingerprinting

❑ Contact your nearest Maryland State Police (MSP) Barracks to determine when applicant/employment fingerprinting is being done.

❑ Report to the barracks on the day of the week and time when applicant/

❑ Employment fingerprinting is being performed. Some local law enforcement agencies will do applicant/employment fingerprinting but you should check with the local law enforcement agency in advance.

❑ Bring a check or money order payable to the MSP (amounts vary throughout the state). MSP will not accept cash for this service.

❑ Following the instruction sheet for the CJIS Form #012 and complete the applicant section of the fingerprint card. Clearly print your information where requested on both sides of the fingerprint card using **black** ink.

❑ Return the fingerprint card to your office for mailing to the Maryland State Board of Elections.

Submission of the Fingerprint Cards and Payment

❑ Mail fingerprint card(s) to the State Board of Elections in a sealed envelope to the attention of | Janey Hegarty and we will forward them to the Criminal Justice Information System — Central Repository (CJIS-CR) for processing.

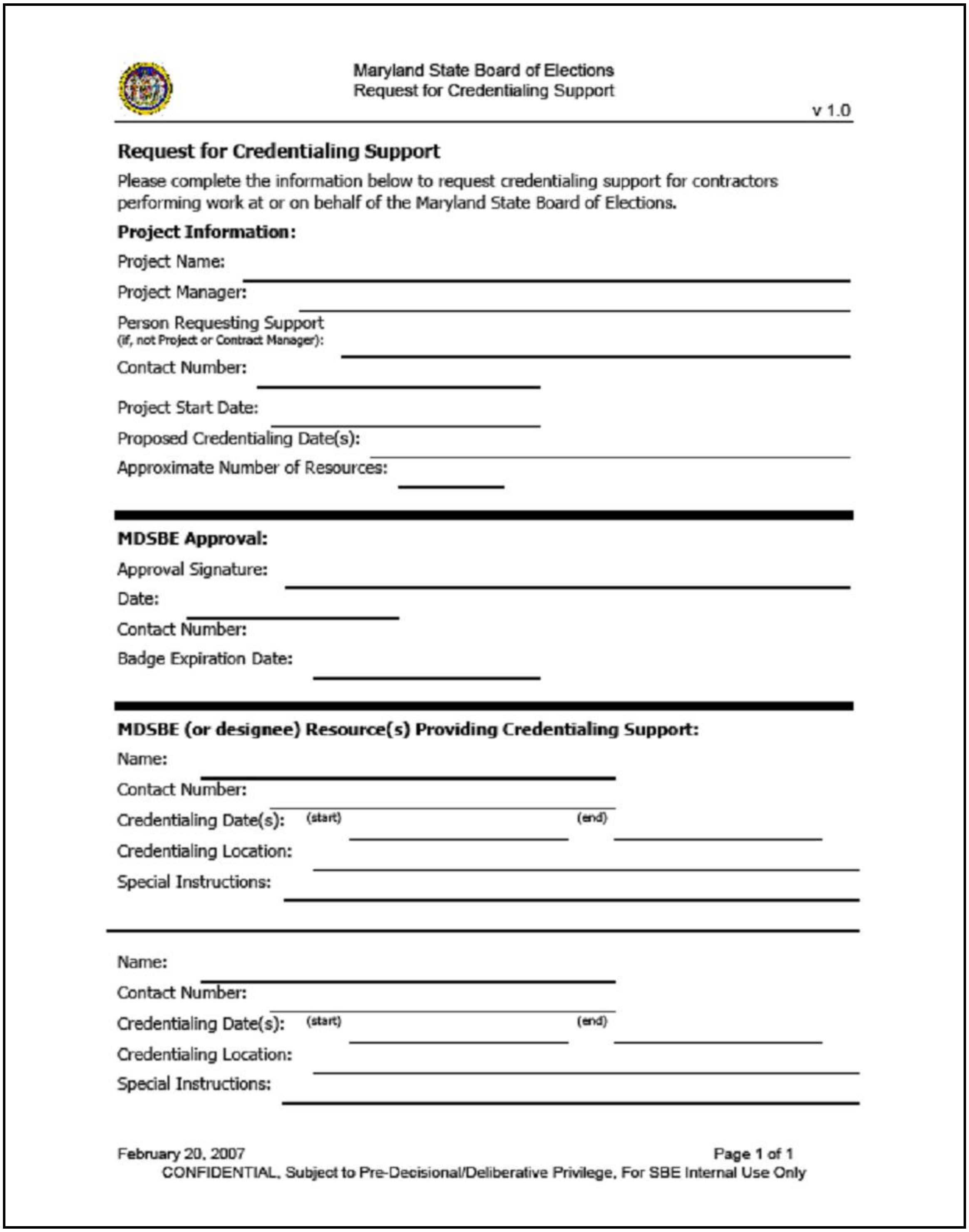
❑ Following completion of the criminal history check and when billed by CJIS-CR, SBE will invoice your local board for the cost of the criminal history check. The cost for the criminal history check is $18.00. A copy of the findings will be provided for your files.

Out-of-State/Contractor or Sub-Contractor Information

❑ If an individual has not been a resident of the State of Maryland for 3^+ years the background check must be completed through their home state or the FBI with the original being forwarded to SBE. A copy should be retained for your files.

If you have any questions regarding this procedure, please call Janey Hegarty/SBE at 410/269-2918.

APPENDIX C – REQUEST FOR CREDENTIALING SUPPORT



Maryland State Board of Elections
Request for Credentialing Support

v 1.0

Request for Credentialing Support

Please complete the information below to request credentialing support for contractors performing work at or on behalf of the Maryland State Board of Elections.

Project Information:

Project Name: ____________________

Project Manager: ____________________

Person Requesting Support
(if, not Project or Contract Manager): ____________________

Contact Number: ____________________

Project Start Date: ____________________

Proposed Credentialing Date(s): ____________________

Approximate Number of Resources: __________

MDSBE Approval:

Approval Signature: ____________________

Date: ____________________

Contact Number:

Badge Expiration Date: ____________________

MDSBE (or designee) Resource(s) Providing Credentialing Support:

Name: ____________________

Contact Number: ____________________

Credentialing Date(s): (start) ____________________ (end) ____________________

Credentialing Location: ____________________

Special Instructions: ____________________

Name: ____________________

Contact Number: ____________________

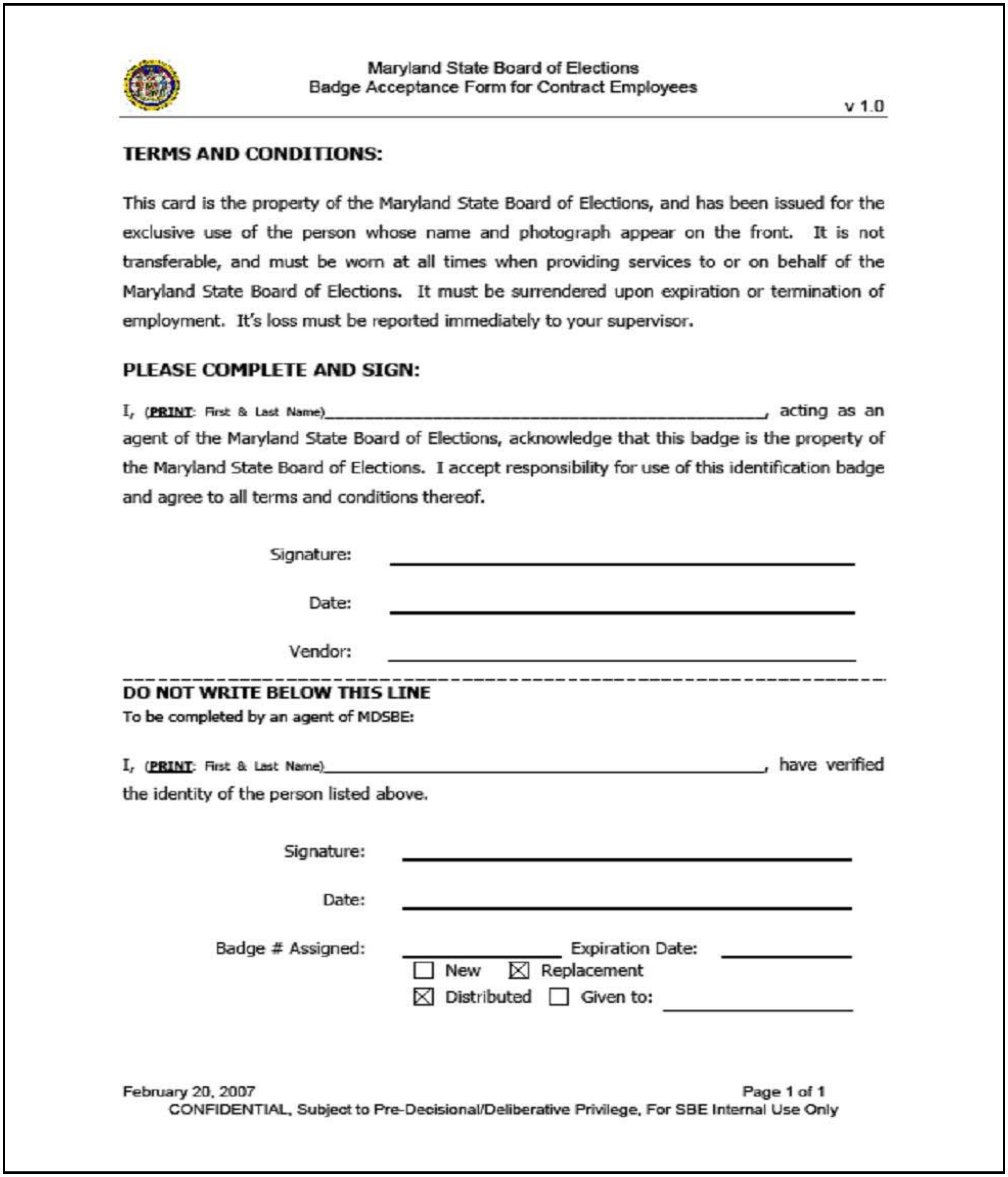
Credentialing Date(s): (start) ____________________ (end) ____________________

Credentialing Location: ____________________

Special Instructions: ____________________

February 20, 2007 Page 1 of 1
CONFIDENTIAL, Subject to Pre-Decisional/Deliberative Privilege, For SBE Internal Use Only

APPENDIX D – BADGE ACCEPTANCE FORM FOR CONTRACTORS



Maryland State Board of Elections
Badge Acceptance Form for Contract Employees

v 1.0

TERMS AND CONDITIONS:

This card is the property of the Maryland State Board of Elections, and has been issued for the exclusive use of the person whose name and photograph appear on the front. It is not transferable, and must be worn at all times when providing services to or on behalf of the Maryland State Board of Elections. It must be surrendered upon expiration or termination of employment. It's loss must be reported immediately to your supervisor.

PLEASE COMPLETE AND SIGN:

I, (**PRINT**: First & Last Name)____, acting as an agent of the Maryland State Board of Elections, acknowledge that this badge is the property of the Maryland State Board of Elections. I accept responsibility for use of this identification badge and agree to all terms and conditions thereof.

Signature: ____

Date: ____

Vendor: ____

DO NOT WRITE BELOW THIS LINE

To be completed by an agent of MDSBE:

I, (**PRINT**: First & Last Name)____, have verified the identity of the person listed above.

Signature: ____

Date: ____

Badge # Assigned: ______________ Expiration Date: ____________

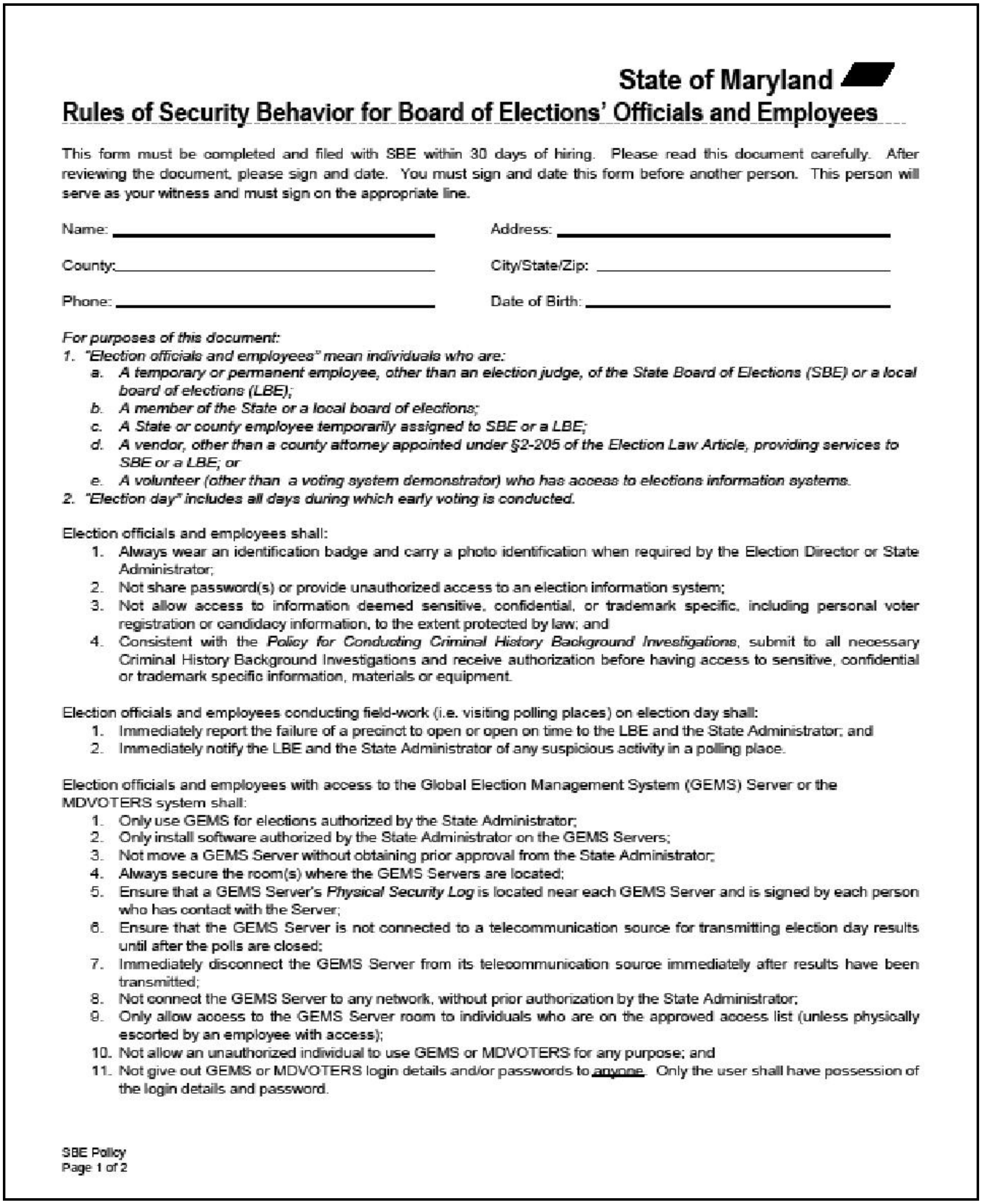
□ New ☒ Replacement

☒ Distributed □ Given to: ______________

February 20, 2007 Page 1 of 1

CONFIDENTIAL, Subject to Pre-Decisional/Deliberative Privilege, For SBE Internal Use Only

APPENDIX E – RULES OF SECURITY BEHAVIOR



State of Maryland

Rules of Security Behavior for Board of Elections' Officials and Employees

This form must be completed and filed with SBE within 30 days of hiring. Please read this document carefully. After reviewing the document, please sign and date. You must sign and date this form before another person. This person will serve as your witness and must sign on the appropriate line.

Name: ______________________ Address: ______________________

County: ______________________ City/State/Zip: ______________________

Phone: ______________________ Date of Birth: ______________________

For purposes of this document:

1. "Election officials and employees" mean individuals who are:

a. A temporary or permanent employee, other than an election judge, of the State Board of Elections (SBE) or a local board of elections (LBE);

b. A member of the State or a local board of elections;

c. A State or county employee temporarily assigned to SBE or a LBE;

d. A vendor, other than a county attorney appointed under §2-205 of the Election Law Article, providing services to SBE or a LBE; or

e. A volunteer (other than a voting system demonstrator) who has access to elections information systems.

2. "Election day" includes all days during which early voting is conducted.

Election officials and employees shall:

1. Always wear an identification badge and carry a photo identification when required by the Election Director or State Administrator;
2. Not share password(s) or provide unauthorized access to an election information system;
3. Not allow access to information deemed sensitive, confidential, or trademark specific, including personal voter registration or candidacy information, to the extent protected by law; and
4. Consistent with the *Policy for Conducting Criminal History Background Investigations*, submit to all necessary Criminal History Background Investigations and receive authorization before having access to sensitive, confidential or trademark specific information, materials or equipment.

Election officials and employees conducting field-work (i.e. visiting polling places) on election day shall:

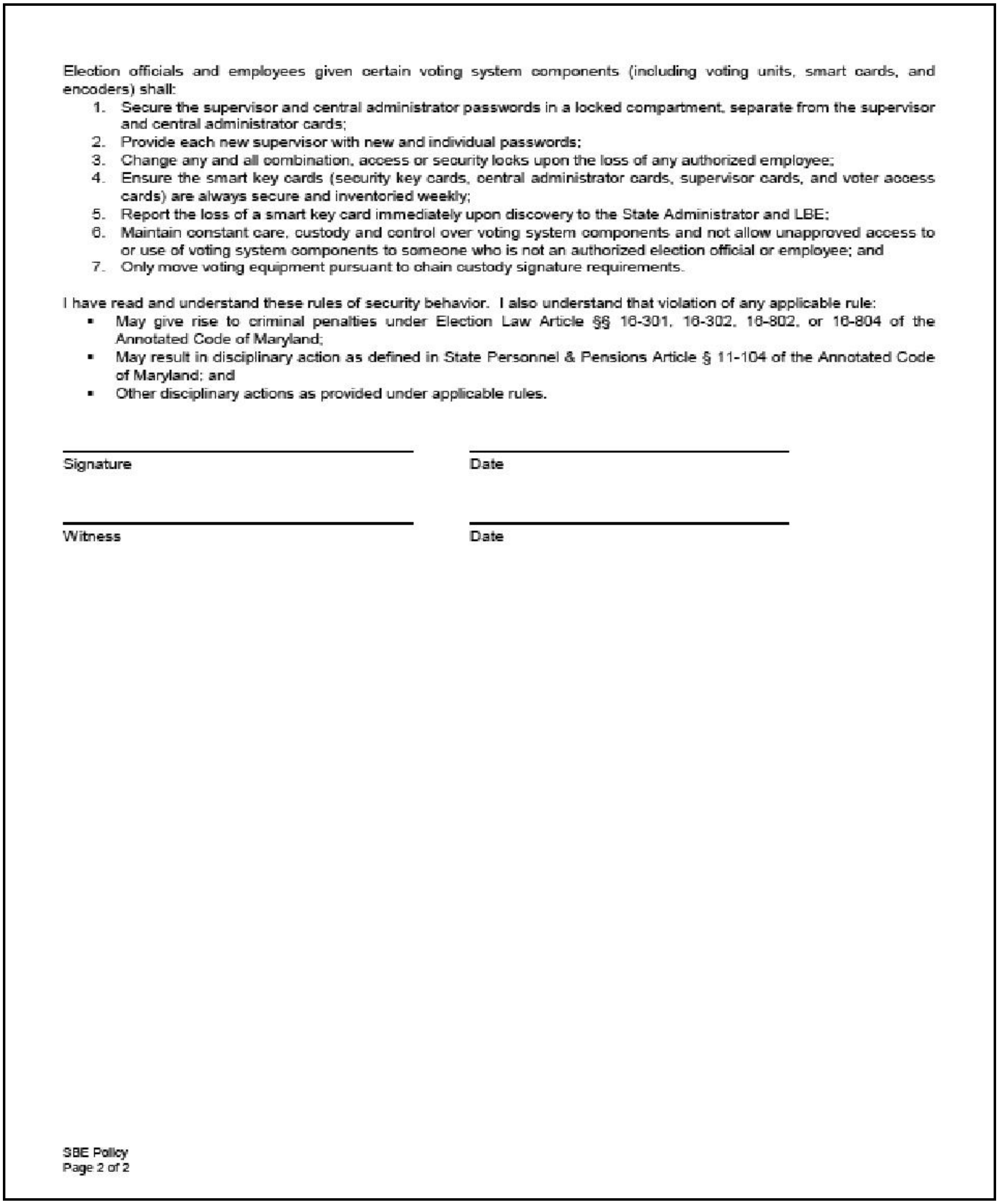
1. Immediately report the failure of a precinct to open or open on time to the LBE and the State Administrator; and
2. Immediately notify the LBE and the State Administrator of any suspicious activity in a polling place.

Election officials and employees with access to the Global Election Management System (GEMS) Server or the MDVOTERS system shall:

1. Only use GEMS for elections authorized by the State Administrator;
2. Only install software authorized by the State Administrator on the GEMS Servers;
3. Not move a GEMS Server without obtaining prior approval from the State Administrator;
4. Always secure the room(s) where the GEMS Servers are located;
5. Ensure that a GEMS Server's *Physical Security Log* is located near each GEMS Server and is signed by each person who has contact with the Server;
6. Ensure that the GEMS Server is not connected to a telecommunication source for transmitting election day results until after the polls are closed;
7. Immediately disconnect the GEMS Server from its telecommunication source immediately after results have been transmitted;
8. Not connect the GEMS Server to any network, without prior authorization by the State Administrator;
9. Only allow access to the GEMS Server room to individuals who are on the approved access list (unless physically escorted by an employee with access);
10. Not allow an unauthorized individual to use GEMS or MDVOTERS for any purpose; and
11. Not give out GEMS or MDVOTERS login details and/or passwords to anyone. Only the user shall have possession of the login details and password.

SBE Policy
Page 1 of 2

Appendix E – RULES OF SECURITY BEHAVIOR, cont'd



Election officials and employees given certain voting system components (including voting units, smart cards, and encoders) shall:

1. Secure the supervisor and central administrator passwords in a locked compartment, separate from the supervisor and central administrator cards;
2. Provide each new supervisor with new and individual passwords;
3. Change any and all combination, access or security locks upon the loss of any authorized employee;
4. Ensure the smart key cards (security key cards, central administrator cards, supervisor cards, and voter access cards) are always secure and inventoried weekly;
5. Report the loss of a smart key card immediately upon discovery to the State Administrator and LBE;
6. Maintain constant care, custody and control over voting system components and not allow unapproved access to or use of voting system components to someone who is not an authorized election official or employee; and
7. Only move voting equipment pursuant to chain custody signature requirements.

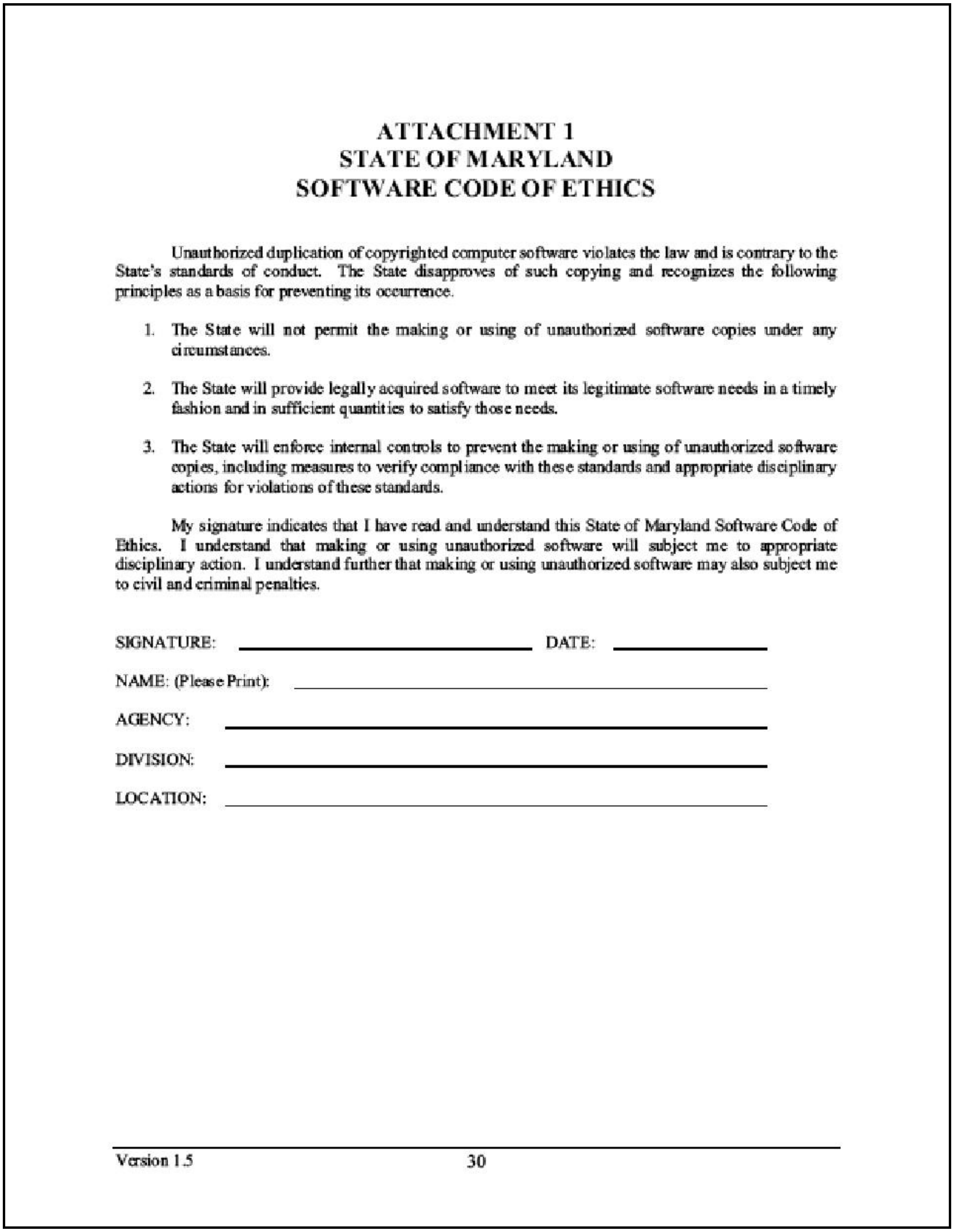
I have read and understand these rules of security behavior. I also understand that violation of any applicable rule:

- May give rise to criminal penalties under Election Law Article §§ 16-301, 16-302, 16-802, or 16-804 of the Annotated Code of Maryland;
- May result in disciplinary action as defined in State Personnel & Pensions Article § 11-104 of the Annotated Code of Maryland; and
- Other disciplinary actions as provided under applicable rules.

Signature	Date
Witness	Date

SBE Policy
Page 2 of 2

APPENDIX F – SOFTWARE CODE OF ETHICS



ATTACHMENT 1
STATE OF MARYLAND
SOFTWARE CODE OF ETHICS

Unauthorized duplication of copyrighted computer software violates the law and is contrary to the State's standards of conduct. The State disapproves of such copying and recognizes the following principles as a basis for preventing its occurrence.

1. The State will not permit the making or using of unauthorized software copies under any circumstances.
2. The State will provide legally acquired software to meet its legitimate software needs in a timely fashion and in sufficient quantities to satisfy those needs.
3. The State will enforce internal controls to prevent the making or using of unauthorized software copies, including measures to verify compliance with these standards and appropriate disciplinary actions for violations of these standards.

My signature indicates that I have read and understand this State of Maryland Software Code of Ethics. I understand that making or using unauthorized software will subject me to appropriate disciplinary action. I understand further that making or using unauthorized software may also subject me to civil and criminal penalties.

SIGNATURE: ______________________ DATE: ____________

NAME: (Please Print): ______________________

AGENCY: ______________________

DIVISION: ______________________

LOCATION: ______________________

Version 1.5 30