

## DOA Financial Security Procedures

### I. PURPOSE:

The purpose of this policy is to protect confidential and sensitive online cash management data from malicious digital cyber-attacks, which includes accessing, changing or deleting sensitive data as well as gaining access to online banking modules for the purpose of stealing or manipulating cash assets.

### II. CYBERSECURITY PLAN:

DOA's Office of Technology Services (OTS) has updated the State's Information Security Policy (ISP) to include a new policy section entitled "Agency Cash Management Services". This policy section clearly addresses the roles and responsibilities related to technical safeguards required for the protection of cash assets of the State. DOA performs all operational processes in compliance with the ISP.

### III. APPLICABILITY:

This policy applies to all DOA employees requiring access to bank accounts, as well as IT related equipment and devices comprising the DOA's network.

All users will be required to review and sign the appropriate Acknowledgment Form.

### IV. RESPONSIBILITIES:

DOA Management is responsible for the plan's maintenance and enforcement. DOA Administrator is responsible for assigning administrative rights and controls. The Administrator will respond to and resolve security issues. Everyone with access to online bank accounts is responsible for adhering to this policy.

### V. SAFEGUARDS OVER CASH MANAGEMENT:

All DOA bank accounts will have the following safeguards in place. If any exceptions are needed for business purposes, approval will be properly documented and requested from Cash Management Review Board (CMRB).

- ACH Debit blocks will be utilized on all Zero-Balance Accounts (ZBAs).
- Post No Checks services, if available, will be utilized on all Deposit Only Accounts.
- Positive Pay services, if available, are required for all bank accounts disbursing funds via check.
- Wires or ACHs will not be sent from any ZBA accounts.
- All ACH files will be dated at least one day after the file is transmitted to the bank.
- ZBAs will be required to have at least two security administrators.
- All limits set will be approved by CMRB and any changes will be addressed by CMRB.
- Third parties will only be allowed view or read only access to DOA bank accounts.
- Department of Treasury will be authorized viewers and signers on all ZBA and Regional bank accounts to allow the bank to accept instruction from Treasury to carry out the powers and policies of CMRB.
- Department of Treasury will be authorized viewers of all ZBAs.

The following are requirements for all DOA employees with access to online cash assets:

- Attend online cyber training presented by JPMorgan Chase on an annual basis.
- Multi-factor authentication must be used when accessing online bank accounts.
- Banking information must be kept confidential and only provided to others when absolutely necessary.

- All user ids, passwords, and multi-factor authentications shall not be shared with others.
- Users shall use caution when clicking on any links in emails or other messages.
- All payment information, including any changes, should always be validated and documented before making the payment or the change in accordance with standard procedures.
- Any information banking or payment related sent via email should only be sent if encrypted.
- The administrator shall be notified of any issues or potential issues

All bank accounts that have been dormant for more than 12 months will be closed and Cash Management Review Board (CMRB) shall be notified.

All bank accounts will be reconciled within a timely manner.

**VI. EXCEPTIONS:**

If any exceptions are needed for business purposes, approval will be properly documented and requested from Cash Management Review Board.

**VII. QUESTIONS:**

All questions regarding this policy should be directed to the administrator.

# DOA FINANCIAL SECURITY PROCEDURES

## EMPLOYEE ACKNOWLEDGMENT

My signature hereon acknowledges that:

- 1) I have received a copy of DOA's Financial Security Procedures;
- 2) I have read this Plan;
- 3) I understand the content of this Plan;
- 4) I agree to comply with the terms and provisions of this Plan;
- 5) I understand that compliance with this Plan is a condition of employment/continued employment; and
- 6) I understand that disciplinary action, including the possibility of termination, will be imposed for violating the terms and conditions of this Plan.

\_\_\_\_\_  
DATE

\_\_\_\_\_  
EMPLOYEE (Signature)

\_\_\_\_\_  
EMPLOYEE (Printed Name)

# DOA FINANCIAL SECURITY PROCEDURES

## ADMINISTRATOR ACKNOWLEDGMENT

My signature hereon acknowledges that:

- 1) I have received a copy of DOA's Financial Security Procedures;
- 2) I have read this Plan;
- 3) I understand the content of this Plan;
- 4) I agree to comply with the terms and provisions of this Plan;
- 5) I understand that compliance with this Plan is a condition of employment/continued employment; and
- 6) I understand that disciplinary action, including the possibility of termination, will be imposed for violating the terms and conditions of this Plan.

\_\_\_\_\_  
DATE

\_\_\_\_\_  
ADMINISTRATOR (Signature)

\_\_\_\_\_  
ADMINISTRATOR (Printed Name)

# DOA FINANCIAL SECURITY PROCEDURES

## MANAGEMENT ACKNOWLEDGMENT

My signature hereon acknowledges that:

- 1) I have received a copy of DOA's Financial Security Procedures;
- 2) I have read this Plan;
- 3) I understand the content of this Plan;
- 4) I agree to comply with the terms and provisions of this Plan;
- 5) I understand that compliance with this Plan is a condition of employment/continued employment; and
- 6) I understand that disciplinary action, including the possibility of termination, will be imposed for violating the terms and conditions of this Plan.

\_\_\_\_\_  
DATE

\_\_\_\_\_  
MANAGEMENT (Signature)

\_\_\_\_\_  
MANAGEMENT (Printed Name)

# DOA FINANCIAL SECURITY PROCEDURES

## ACCOUNT SIGNER ACKNOWLEDGMENT

My signature hereon acknowledges that:

- 1) I have received a copy of DOA's Financial Security Procedures;
- 2) I have read this Plan;
- 3) I understand the content of this Plan;
- 4) I agree to comply with the terms and provisions of this Plan;
- 5) I understand that compliance with this Plan is a condition of employment/continued employment; and
- 6) I understand that disciplinary action, including the possibility of termination, will be imposed for violating the terms and conditions of this Plan.

\_\_\_\_\_  
DATE

\_\_\_\_\_  
SIGNER (Signature)

\_\_\_\_\_  
SIGNER (Printed Name)