CYBERSECURITY PLAN AND FINANCIAL SECURITY PROCEDURES

Related to the Management of Cash Assets

EMPLOYEE ACKNOWLEDGMENT

Employees are responsible for:

Complying with the approved Cybersecurity Plan and Financial Security Procedures and taking reasonable steps to protect OLG/DCRT computer systems and network.

Completing required online IT security awareness training programs.

Ensuring full protection of all assigned user ids and passwords and bank security tokens.

Exercising caution when opening suspicious emails with links and/or attachments.

Passing periodic simulated phishing tests or similar criminal attempts to compromise the agency's financial security of cash management.

Notifying IT immediately of any virus/malware/ransomware transmitted to computer.

Employees are required to immediately close websites used for bank account access after logging off and to logoff OLG/DCRT network at the end of each workday.

My signature hereon acknowledges that:

1) I have received a copy of the OLG/DCRT Cybersecurity Plan and 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;

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)

DATE _____