SAVE FORM

SELF ASSESSMENT OF INTERNAL CONTROL

Form K

Budget and Financial Cycles

Computer Security Cycle

Department _____

Fiscal Year Ending _____ ☐ NA-_____

		Yes	No	N/A	Comments
	A. Control Activities / Information and Communications				
1.	Is there a formal organizational chart which identifies the individuals responsible for the: a. Computer systems? b. Computer security?				
2.	Has management considered the appropriate segregation of duties among personnel involved in the IT security function?				
3.	Have roles and responsibilities been clearly defined and communicated?				
4.	Is the financial system's business owner management appropriately included in the design of the IT security function from a data ownership?				
5.	Does management have a controlled process in place to update the security policy and procedure documentation on a periodic basis?				
6.	Is a formal documented security administration process in place to ensure that all applications access, including restricted access to financial applications, is approved? (Critical Control)				
7.	Has management implemented a formal process for changing financial data file permissions?				
8.	Has management implemented a formal security administration process for granting, changing, and removing direct access to financial data?				
9.	Does management periodically review monitoring reports to identify potential unauthorized activity? (Critical Control)				
10.	When an employee or contractor is terminated, are the following precautions implemented immediately: a. The employee or contractor is denied access to the equipment? b. The employee or contractor is denied access to any data, program listing, etc.? c. All other employees are informed of the employee's termination?				

Computer Security Cycle

		Yes	No	N/A	Comments
	d. The employee or contractor's user-id and password are deleted from the computer system?				
11.	Is there a time out/screen saver and/or log off function, which will protect a terminal if left unattended?				
12.	Does a login name and a password uniquely identify users when they sign on to the system (e.g. no group users IDs)?				
13.	If an employee incorrectly enters their password three times in a row, does the computer system deny them access to the computer system until reset by the system administrator?				
14.	Do all PCs under control of the agency use a recognized anti-virus (A/V) or end-point security program? Does the agency run the A/V program on a regular schedule?				
15.	Does the agency have a firewall established for their Lan or for individual workstations?				
16.	Is there a written disaster recovery (DR) plan?				
17.	Does the DR plan include identification of the following? a. Critical applications? (Critical Control) b. Staff responsibilities? (Critical Control) c. Steps for recovery of the system? (Critical Control) d. Computer equipment needed for temporary processing? (Critical Control) e. Business location(s) that could be used to process critical applications in the event of an emergency? (Critical Control)				
18.	Has the agency taken steps to prevent and minimize potential damage and interruption through the use of data and program backup procedures including off-site storage of backup data as well as environmental controls, staff training, and hardware maintenance and management? (Critical Control)				
19.	Are there provisions for retaining and/or copying master files, and is there practical means of reconstruction a damaged or destroyed file**?**				

Computer Security Cycle

		Yes	No	N/A	Comments
	B. Monitoring				
20.	Does the agency monitor information systems access, investigates apparent violations, and takes appropriate remedial and disciplinary action? (Critical Control)				
21.	Does the department or management balance control totals generated during computer processing with those originally established and reconcile all discrepancies? (Critical Control)				