|  |
| --- |
| Agency: Click here to enter text. |
| Preparer(s): Click here to enter text. | Date: Click here to enter text. |

Risks: Controls over information technology are not adequate to ensure: access to IT systems and electronic data is reasonable and restricted to authorized individuals; transactions and activities related to IT systems are properly authorized; output is accurate, complete and valid; privacy and security of sensitive data is adequately addressed; and IT systems are available to meet business needs.

Note: for purposes of this checklist, please consider agency administered applications, agency desktop support and agency retained electronic data.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| YES | NO | \*N/A |  | CHECKLIST QUESTION |
| □ | □ | □ | 1. | Are appropriate staff members familiar with the policies of the state’s Chief Information Officer? <https://ocio.wa.gov/policies>  |
| □ | □ | □ | 2. | Has an IT risk assessment been conducted and documented within the past two years? If so, are progress updates conducted/documented annually?  |
| □ | □ | □ | 3. | Does a business continuation plan exist which identifies critical activities, backup files, programs, and alternative processing sites? |
| □ | □ | □ | 4. | Have change management procedures been established and documented for version control and revisions to agency IT applications? |
| □ | □ | □ | 5. | Are system security and application access logs enabled and reviewed periodically for unauthorized access and anomalies? |
| □ | □ | □ | 6. | Are backups of operating systems, critical data, and key software programs made on a regular basis and stored at an off-site location? |
| □ | □ | □ | 7. | Are initial access requests to IT systems, and their subsequent approval, authorized and documented? |
| □ | □ | □ | 8. | Are strong password settings enforced for all agency systems (interval change, minimum length, lock out, etc.)? |
| □ | □ | □ | 9. | Are documented requirements in place for periodic review/modification/removal of user access agency IT systems when an employee leaves or is assigned to a different role? |
| □ | □ | □ | 10. | Is sensitive/restricted data (on networks, personal computers, and back up media), classified and protected by restricted access, encryption, or other controls? |
| □ | □ | □ | 11. | Does agency policy require users to have individual accounts and passwords and are the users prohibited from sharing those passwords? |
| □ | □ | □ | 12. | Is the agency’s policy on acceptable use of computer resources periodically communicated to all employees including new hires? |
| □ | □ | □ | 13. | Is antivirus software installed, operating and being updated for all computing resources (laptops, desktops, servers, etc)? |
| □ | □ | □ | 14. | Is system administrator access to the production systems restricted and based on need? |
| □ | □ | □ | 15. | Are policies and procedures in place allowing management to adequately and efficiently detect and contain IT security incidents? |
| □ | □ | □ | 16. | Are procedures in place to apply security updates and patches for all servers, workstations, and portable computers? |

\*N/A - Not Applicable

Comments/Compensating Controls:

………………………………………………………………………………………………………………………………

………………………………………………………………………………………………………………………………

………………………………………………………………………………………………………………………………

………………………………………………………………………………………………………………………………

Monitoring – ongoing/separate evaluations:

………………………………………………………………………………………………………………………………

………………………………………………………………………………………………………………………………

………………………………………………………………………………………………………………………………

………………………………………………………………………………………………………………………………

Summary:

………………………………………………………………………………………………………………………………

………………………………………………………………………………………………………………………………

………………………………………………………………………………………………………………………………

………………………………………………………………………………………………………………………………