DIRECTIVE 1: INFORMATION TECHNOLOGY INTERNAL CONTROLS FORM

Each agency should complete and submit this form. Agencies may find it helpful to refer to Citywide Application Security Policy and Security Standards before completing this form.

* Required

1. Agency: *

2. Name: *

3. Title: *

4. Email: *

5. Does your Agency have an individual serving as Chief Information Officer (CIO)? *

- ◯ Yes
- ◯ No

6. If yes, please provide their name and email address.

7. If not, please advise when this will be rectified.

8. Has your agency designated a Chief Information Security Officer (CISO) or equivalent officer? *

- ◯ Yes
- ◯ No

9. If yes, please provide their name and email address.

10. If not, please advise when this will be rectified.

11. Does your Agency CISO and/or CIO partner with agency employees, consultants, federal and state agencies, OTI, and the New York City Cyber Command to ensure understanding of and adherence to the Citywide Information Security Policies? *

- ◯ Yes
- ◯ No

12. If not, please provide an explanation why this does not occur.

13. Does your Agency's IT leadership maintain a long-range Strategic Plan, including projects, milestones and timelines for completion? *

- ◯ Yes
- ◯ No

14. If not, please provide an explanation why this does not occur.

15. Does your Agency establish a Project Steering Committee to review and monitor each project's progress? *

- ◯ Yes
- ◯ No

16. If yes, please briefly explain the Committee's function.

17. If not, please explain why not and explain how each project is monitored.

18. How are computer processing services provided within the agency? Please check all that apply. *

- ☐ OTI
- ☐ FISA
- ☐ Agency personnel
- ☐ Vendors/consultants
- ☐ Other

19. Does your Agency conduct internal Information Technology audits? *

- ◯ Yes
- ◯ No

20. If yes, what areas/systems have been audited internally since the last Directive 1 filing with the Comptroller's Office?

21. If not, how does the agency ensure Citywide mandates, policies and procedures are complied with?

22. Has your Agency's IT systems or security been audited by an external auditor since the last Directive 1 filing with the Comptroller's Office? *

- ◯ Yes
- ◯ No

23. If yes, please provide a list of findings and the status of related recommendations (implemented, pending, not implemented)

24. Does your Agency maintain a list of all applications and systems in use at the Agency? *

- ◯ Yes
- ◯ No

25. If yes, please upload a list of applications and systems, including the following for each: Application Name, Description, URL (if applicable), Data Classification (Public, Private, Sensitive, Confidential), Internal or Public Facing Indicator, Non-restricted, Sensitive and Restricted

26. If not, please advise why not and when this will be rectified.

27. Does the agency have adequate controls in place to ensure that all business owners and all systems fully comply with Citywide Application Security Policy and Citywide Application Security Standards? *

- ◯ Yes
- ◯ No

28. If yes, please explain how and when this was assessed.

29. If not, please explain how and when all issues will be rectified.

30. Does the agency have adequate controls in place to ensure that all systems which collect and maintain personal identifiable information (PII) and/or personal health information (PHI) preserve the security and privacy of information in full compliance with all applicable legal requirements? *

- ◯ Yes
- ◯ No

31. If yes, please briefly explain how this is accomplished.

32. If not, please explain why not and provide a plan for correcting this.

33. Does the agency have policies and procedures in place to ensure that all new systems are tested for performance and stability in a non-production environment before moving them into production? *

- ◯ Yes
- ◯ No

34. If yes, please briefly explain how this is accomplished.

35. If not, please explain when this will be rectified.

36. Does the agency have policies and procedures in place to ensure that all new systems comply with all Citywide information policies and standards before they are moved into production? *

- ◯ Yes
- ◯ No

37. If yes, please briefly explain how this is accomplished.

38. If not, please explain when this will be rectified.

39. Does the agency ensure the CISO (or equivalent) approves all application security which has an agency level impact before implementation? *

- ◯ Yes
- ◯ No

40. If yes, please briefly describe the process.

41. If not, please explain why not and when this will be rectified.

42. Were all applications which were newly developed or upgraded since the last Directive 1 filing with the Comptroller's Office, approved for use at the Agency by the Chief Information Officer (CIO, or equivalent position) prior to migration to production environment? *

- ◯ Yes
- ◯ No

43. Do the agency's web services and distributed components of City applications that collect and store data comply with the requirements of the Citywide Information Policy and Standard? *

- ◯ Yes
- ◯ No

44. If yes, please explain how this was assessed.

45. If not, please explain how this will be rectified.

46. Do all agency applications subject to spam or forms-based denial of service (DOS) attacks employ CAPTCHA or equivalent technology? *

- ◯ Yes
- ◯ No

47. If not, please how when this will be rectified.

48. Does the agency use an approved source code repository (for local/on premise and cloud-based NYC3 approved applications) with check-in and check-out capabilities for all City developed applications? *

- ◯ Yes
- ◯ No

49. If yes, please explain how and when this was assessed.

50. If not, please explain when and how this will be rectified.

51. Are new systems developed in accordance with OTI's Project Management Life Cycle (PMLC) and/or NYC Project Standards? *

- ◯ Yes
- ◯ No

52. If yes, please list all new systems developed since the last Directive 1 filing with the Comptroller's Office.

53. If not, please explain what standards are used by the agency in lieu of these.

54. Are there adequate controls in place to ensure the agency fully complies with Comptroller's Directive 31 when handling IT consultants and IT professional services payment requests? *

- ◯ Yes
- ◯ No

55. If yes, please briefly describe these processes.

56. If not, please explain when this will be rectified.

57. Does the agency have adequate controls in place to safeguard all IT assets against loss and theft? *

- ◯ Yes
- ◯ No

58. If yes, please briefly explain how and when this was last assessed.

59. If not, please explain how and when this will be rectified.

60. Has the Annual CSP report and Certification process been completed?

- ◯ Yes
- ◯ No

61. If yes, please submit the report and certification to the Comptroller's Office with the Financial Integrity Statement. If not, please explain when it will be completed?

62. Please sign this form in the space below. This signature confirms the accuracy of responses provided above. *