APPENDIX F1: Sample Fraud Control Policy Framework

*The information in this appendix can serve as an outline of the key elements to be considered in drafting a fraud control policy.*

1. Policy Statement
2. Management’s statement regarding fraud tolerance or attitude about fraud
3. Management’s commitment to ethical business practices
4. Definitions
5. Definition of fraud
6. Definitions of other referenced terms
7. Fraud Control Strategy
8. Roles and responsibilities
   1. Board of Directors
   2. Executive or Senior Management
      1. Fraud Control Officer
   3. Legal Department
   4. Human Resources Department
   5. Internal Audit Department
   6. Other management and employees
9. Elements of management’s fraud risk management program
   1. Fraud risk governance
   2. Fraud risk assessment
   3. Fraud prevention and detection
   4. Fraud investigations and corrective action
   5. Fraud monitoring
10. Relationship to Code of Business Conduct and other relevant corporate policies (i.e., employee handbook, conflicts of interests, FCPA / anti-corruption compliance policy, expense reimbursements, etc.)
11. Fraud Risk Assessment
12. Fraud risk assessment objectives
13. Fraud risk assessment methodology
14. Fraud risk assessment participants
15. Management’s response to fraud risk assessment results
16. Fraud Prevention and Detection Controls
17. Business process control activities
18. Physical access control activities
19. Logical access control activities
20. Transaction control activities
21. Technological control activities
22. Conflicts of Interest
23. Human Resource procedures
    1. Pre-employment screening
    2. Periodic screening activities
    3. Compensation and performance measures
    4. Training
    5. Exit interviews
24. Segregation of duties
25. Authority and responsibility limits
26. Fraud Detection procedures
27. Data analytics
28. Whistleblower systems
29. Fraud Reporting
30. Reporting requirements for management and employees
    1. Examples of types of issues to be reported
31. Channels for reporting concerns, complaints or violations
    1. Hotline
    2. Website
    3. Electronic mail (“email”) address
    4. Letters to board of directors or designated personnel
    5. Chain-of-command
    6. Open door policy
32. Anonymous reporting vs. confidentiality reporting
33. Anti-retaliation or whistleblower protection statement for personnel who report concerns, complaints or violations of fraud
34. Reporting by third parties
35. Fraud Investigation Procedures
36. Evaluation of reports
37. Escalation of reports
38. Retention of reports
39. Investigation resources
40. Investigation protocols
41. Communicating investigation results
42. Disciplinary action
43. Corrective action
44. Recovery and restitution
45. Evaluation of investigation performance
46. Fraud Monitoring Activity
47. Areas of fraud monitoring evaluation
48. Scope and frequency of fraud monitoring evaluation activities
49. Fraud monitoring evaluation criteria
50. Sources of information (or “data inputs”) for fraud monitoring evaluation activities
51. Communicating results of fraud monitoring evaluation activities